الحماية الجنائية للأمن الالكتروني

دكتور

حازم حسن الجمل

دكتوراه في الحقوق - جامعة المنصورة

دار الفكر والقانون

١ شارع الجلاء - أمام بوابة الجامعة

المنصورة - برج آية

تليفون: ٠٥٠/٢٢٣٦٢٨١ محمول: ٠١٠٠٦٠٥٧٧٦٨

الحماية الجنائية للأمن الالكترونى

دكتور

حازم حسن الجمل

دكتوراه في الحقوق

جامعة المنصورة

2015

دار الفكر والقـانون

للنشر والتوزيـع

1 ش الجلاء أمام بوابة الجامعة برج آية

تليفكس : 0020502235671 تليفون : 0502236281

محمول 00201006057768

اسم الكتاب : الحماية الجنائية للأمن الالكتروني

اسم المؤلف: دكتور/ حازم حسن الجمل

الطبعة الأولى

سنة الطبع : 2015

رقم الإيداع بدار الكتب المصرية : 26823

الترقيم الدولي: 9789777170438

الناشر : دار الفكر والقانون للنشر والتوزيع

1 ش الجلاء أمام بوابة الجامعة برج آية

تليفكس : 0020502235671 تليفون : 0502236281

محمول 00201006057768

dar.elfker@Hotmial.com

المحامي / أحمد محمد أحمد سيد أحمد

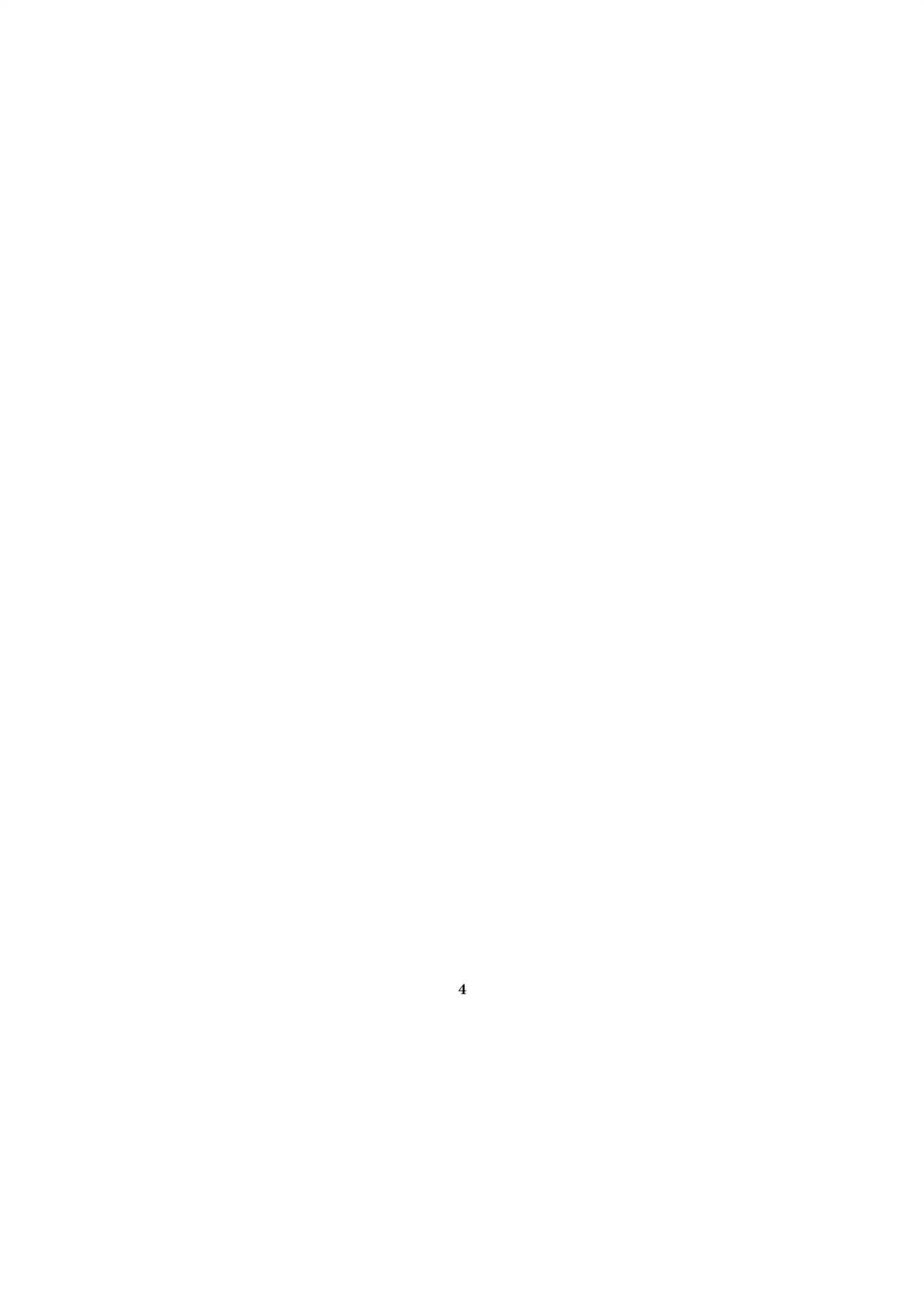
إهـــــــــداء

إلى فقراء هذا العالم ...

إلى روح والدى الساكنة فى الأبدية... إلى أسرتي... إلى ابنتّى هايدى وندي،

فلذتا كبدى وقُرتا عينى ..

د. حازم حسن الجمل



شكر وتقدير وعرفان

فى البداية نشكر المولى عز وجل على عظيم نعمه علينا، وتوفيقه لنا فى إتمام هـذه الدراسة. ثم أتوجه بخالص الشكر والتقدير والعرفـان بأسـمى معـانى الحـب والامتنـان والثناء إلى أستاذى الفاضل العالم الجليل العميد أ.د / أحمـد شـوقى عمـر أبـو خطـوه (أستاذ القانون الجنائى بكلية الحقوق، جامعة المنصورة، وعميد الكلية الأسبق)

د. حازم حسن الجمل



مقـدمـة

أولاً : موضوع الدراسة :

يتعلق موضوع هذه الدراسـة بالحمايـة الجنائيـة (الموضـوعية والإجرائيـة) للأمـن الالكترونى فى التشريع الإماراتي. حيث أصبح الاعتداء على الأمـن الالكـترونى مـن أخطـر الظواهر المستحدثة تأثيرا على أمن الدولة، وعقيـدتها، واقتصـادها، وتراثهـا الحضـاري، والنظام العام فيها، والسلم الاجتماعي، وكذلك العلاقات الدولية والإقليمية[1].

ثانياً : أهمية الدراسة :

تكتسب هذه الدراسة أهميتها من خلال البحث عن مدى قصـور قواعـد الحمايـة الجنائية (الموضوعية والإجرائية) المقررة بموجب المنظومـة التشريعيـة، التـى اسـتهدف بها المشرع الإماراتى حماية الأمـن الالكـتروني، باعتبارهـا مـدخلاً هامـا لمصـالح أساسـية وهامة تشمل أمن الدولة، واقتصادها، وعلاقاتها بين الدول...الخ.

---

(1) أنظر : المادة (14) من مرسوم بقانون اتحادى رقم (3) لسنة 2012م، بإنشـاء الهيئـة الوطنيـة للأمن الإلكتروني، فى دولة الإمارات العربيـة المتحـدة، الصـادر بتـاريخ 2012/8/13م، الجريـدة الرسمية رقم (540)، ص 13.

ثالثاً : مشكلات الدراسة :

تعالج هذه الدراسة كثير من المشكلات ذات الصلة بسياسة ومنهج وخطة المشرع الإماراتى بشأن تجريم، وملاحقة الاعتداء على الأمن الالكتروني. وما كشف عنه بالضرورة الواقع العملى من قصور فى بعض الأحيان، أو عدم التوائم والتناسق التشريعى بين مصادر الحماية الجنائية المختلفة فى أحيان أخري.

رابعاً : أهداف الدراسة :

تهدف هذه الدراسة إلى التعرف على جرائم الاعتداء على الأمن الالكتروني، وخطورتها، وانعكاساتها المختلفة، وكذلك استكشاف أوجه قصور قواعد الحماية الجنائية المقرر فى هذا المجال الحيوي، بهدف التوصل إلى رسم معالم النموذج التشريعى الأمثل للمصالح محل الحماية الجنائية.

خامساً : خطة الدراسة :

فى سبيلى إلى بيان الأهداف المنشودة من هذا البحث، فإن دراستى لهذا الموضوع ستكون على نحو الخطة التالية :

الفصل الأول : التعريف بجرائم الاعتداء على الأمن الالكتروني.

الفصل الثانى : الحماية الجنائية الموضوعية للأمن الالكتروني.

الفصل الثالث : الحماية الجنائية الإجرائية للأمن الالكتروني.

الفصل الأول

التعريف بجرائم الاعتداء على الأمن الالكتروني

فى سبيل التعريف بجرائم الاعتداء على الأمن الالكتروني، يقتضى الأمر أن نبحث فى مفهوم الأمن الالكتروني، ومصادر حمايته القانونية، ثم نعرج بعدها إلى تحديد المصالح محل الحماية الجنائية وسبلها.

المبحث الأول : مفهوم الأمن الالكترونى ومصادر الحماية الجنائية.

المبحث الثانى : تحديد المصالح محل الحماية الجنائية وسبلها.

المبحث الأول

مفهوم الأمن الالكترونى ومصادر الحماية الجنائية

أولاً : مفهوم الأمن الالكترونى :

يقصد بالأمن الالكترونى (تأمين وحماية) الشبكة المعلوماتية، وشبكة الاتصالات، ونظم المعلومات، وعمليات جمع المعلومات، باستخدام أى من الوسائل الإلكترونية[1].

ثانياً : مصادر حماية الأمن الالكترونى فى التشريع الإماراتى :

تعتبر القوانين، والمراسيم التالية، من أهم مصادر الحماية التشريعية للأمن الالكترونى فى دولة الأمارات العربية المتحدة[2] : ـ

- المرسوم بقانون اتحادى رقم (3) لسنة 2012م، بشأن إنشاء الهيئة الوطنية للأمن الالكتروني[3]. وقد نص المشرع الإماراتى بموجب المادة

(1) المادة الأولى من مرسوم بقانون اتحادى رقم (3) لسنة 2012م، بإنشاء الهيئة الوطنية للأمن الإلكتروني.

(2) ينظم الحماية الجنائية للبيئة المعلوماتية فى الولايات المتحدة الأمريكية التشريع الفيدرالى الصادر سنة 1984 المعدل فى السنوات التالية (1986، 1990، 1994، 1996، 2001). وفى فرنسا صدر أول تشريع سنة 1979 لحماية الحريات والمعطيات، وفى سنة 2004 صدر قانون يتعلق بالاقتصاد الرقمي.

(3) صدر بتاريخ 2012/8/13م الموافق 25 رمضان 1433هـ ونشر فى الجريدة الرسمية رقم (540)، ص 13.

رقم (23) من هذا المرسوم على إلغاء كل حكم يخالف أو يتعارض مع أحكام هذا المرسوم بقانون.

- المرسوم بقانون اتحادى رقم (5) لسنة 2012م، فى شأن مكافحة جرائم تقنية المعلومات[1]، وقد ألغى المشرع الإماراتى بموجب المادة رقم (50) من هذا المرسوم القانون الاتحادى رقم (2) لسنة 2006 فى شأن مكافحة جرائم تقنية المعلومات، وكذلك نص صراحة بموجب هذه المادة على إلغاء كل حكم يخالف أو يتعارض مع أحكام هذا المرسوم بقانون.

- القانون الاتحادى رقم (1) لسنة 2006م، فى شأن المعاملات والتجارة الالكترونية[2].

والجدير بالملاحظة أنه رغم التكامل بين المصادر القانونية السالفة البيان فى تقرير الحماية للأمن الالكتروني، إلا أن النص صراحة بموجب هذه القوانين على إلغاء كل حكم يخالف أو يتعارض مع أحكامها، ربما يثير بعض المشكلات المحتملة، خصوصاً عند وجود تعارض بين هذه القوانين - وهى من القوانين الخاصة - وبين القواعد والنصوص العامة، التى تقرر حماية مصلحة جوهرية (موضوعية أو إجرائية) للأمن الالكتروني.

ولدينا فإنه من الأنسب أن يجرى نصوص هذه المواد على النحو التالى :

---

(1) صدر بتاريخ 2012/8/13م الموافق 25 رمضان 1433هـ

(2) صدر بتاريخ 30 ذى الحجة 1426 هـ الموافق 30 يناير 2006م.

".... ولا يسرى فى شأنه أى حكم يتعارض مع أحكامه. بدلاً من النص على أنه :" ... يلغى كل حكم يخالف أو يتعارض مع أحكام هذا المرسوم بقانون".

ثالثاً : مفهوم جرائم الاعتداء على الأمن الالكترونى :

لم نصادف حتى الآن تعريف محدد لجرائم الاعتداء على الأمن الالكتروني، ومن ثم يمكن تعريف هذا النوع من الجرائم، بأنها كافة صور السلوك غير المشرع (الايجابى أو السلبي) الذى يمثل اعتداء (بالضرر أو التهديد به) على كافة سبل تأمين وحماية الشبكة المعلوماتية، وشبكة الاتصالات، ونظام التحكم الالكتروني، ونظم المعلومات، وعمليات جمع المعلومات، أو ما شابه ذلك، والذى يقرر لها المشرع جزاء جنائى أو تدبير احترازي.

رابعاً : التمييز بين جرائم الاعتداء على الأمن الالكترونى وما يتشابه معها :

تتميز جرائم الاعتداء على الأمن الالكتروني، بأنها اعتداء على أمن وحماية شبكة الاتصالات، ونظم المعلومات، ونظم التحكم الالكترونى ذاتها. ويتم هذا الاعتداء بصور مختلفة، تمثل خطورة على مصالح متعددة وهامة. ومن أهم صور هذا الاعتداء الدخول إلى هذه الأنظمة بغير تصريح، أو بتجاوز حدود التصريح، أو البقاء فيه بصورة غير مشروعة، أو

إلغاء، أو حذف، أو تدمير، أو إفشاء، أو إتلاف، أو تغيير، أو تزوير، هذه الأنظمة، أو غير ذلك من صور السلوك الأخرى المشابهة، التى تمثل اعتداء على نظم التأمين، والحماية لهذه الأنظمة الالكترونية.

ومن ثم، فإن جرائم الاعتداء على الأمن الالكترونى تختلف بذلك عن استخدام نظم المعلومات، وشبكة الاتصالات، ونظم التحكم الالكتروني، كأداة أو وسيلة لارتكاب جرائم أخرى. من ذلك مثلا إنشاء موقع الكترونى لنشر معلومات بهدف الترويج لإثارة الفتنة، أو الإضرار بالوحدة الوطنية[1]. أو بهدف الترويج للأسلحة[2]، أو نشر معلومات لجماعة إرهابية[3]، أو الترويج للاتجار بالمخدرات[4]، أو بغرض ارتكاب أفعال جرميه متعلقة بأموال غير مشروعة[5]، أو ما شابه ذلك.

خامساً : خصائص جرائم الاعتداء على الأمن الالكترونى :

يمكن أيجاز أهم الخصائص المميزة لجرائم الاعتداء على الأمن الالكترونى فى النقاط التالية :-

- تمثل جرائم الاعتداء على الأمن الالكتروني، تهديدا صارخا على

(1) المادة (24) مرسوم بقانون اتحادى رقم (5) لسنة 2012 فى شأن مكافحة جرائم تقنية المعلومات.
(2) المادة (25) مرسوم بقانون اتحادى رقم (5) لسنة 2012 فى شأن مكافحة جرائم تقنية المعلومات.
(3) المادة (26) مرسوم بقانون اتحادى رقم (5) لسنة 2012 فى شأن مكافحة جرائم تقنية المعلومات.
(4) المادة (35) مرسوم بقانون اتحادى رقم (5) لسنة 2012 فى شأن مكافحة جرائم تقنية المعلومات.
(5) المادة (37) مرسوم بقانون اتحادى رقم (5) لسنة 2012 فى شأن مكافحة جرائم تقنية المعلومات.

مصالح أساسية فى الدولة، كأمن الدولة، واقتصادها، والنظام العام فيها، والسلم الاجتماعي، وكذلك العلاقات الدولية والإقليمية، لذلك فإن المشرع يعتبر هذه الجرائم من جرائم أمن الدولة[1].

- جرائم الاعتداء على الأمن الالكتروني، جريمة لها بعد دولي، أى أنها جريمة عابرة للحدود أو الأوطان، تتخطى آثارها، ونتائجها، وأضرارها أكثر من دولة فى آن واحد.

- تجمع جرائم الاعتداء على الأمن الالكترونى بين صفة جرائم الضرر الفعلى وجرائم الخطر، أى التهديد بالضرر المحتمل الوقوع. وهذه الأخيرة هى مرحلة مبكرة من الحماية، يستهدف بها المشرع اعتراض خطوات السلوك الإجرامى قبل أن يفضى إلى الضرر.

- جرائم الأمن المعلوماتى تتم فى بيئة رقمية معلوماتية، قوامها النظم البرامجية المعلوماتية الحاسوبية، وأجهزة، ومعدات، وأدوات حاسوبية[2]، أو رقمية.

- جرائم الاعتداء على الأمن الالكتروني، يتميز فاعليها أو مرتكبيها

---

(1) حيث تنص المادة رقم (44) من مرسوم بقانون اتحادى رقم (5) لسنة 2012 فى شأن مكافحة جرائم تقنية المعلومات، على أنه " تعتبر الجرائم الواردة فى المواد 4، .... من هذا المرسوم من الجرائم الماسة بأمن الدولة.

(2) أنظر فى ذلك : خبير/ عبد الناصر محمد محمود فرغلى ، د. محمد عبيد سيف سعيد المسمارى : الإثبات الجنائى بالأدلة الرقمية من الناحيتين القانونية والفنية، دراسة تطبيقية مقارنة، المؤتمر العربى الأول لعلوم الأدلة الجنائية والطب الشرعي، الرياض، 2-4/11/ 1428هـ - الموافق 12-14/11/2007م، ص 11.

وكذلك الشركاء فيها فى أغلب الأحيان بالذكاء[1].

(1) انظر : د. غنام محمد غنام : دور قانون العقوبات فى مكافحة جرائم الكمبيوتر والانترنت وجرائم الاحتيال المنظم باستعمال شبكة الانترنت، دار الفكر والقانون، المنصورة، مصر، 2010، ص15.

المبحث الثاني

تحديد المصالح محل الحماية الجنائية

أولاً : العناصر محل الحماية الجنائية فى مجال الأمن الالكترونى :

تعتبر الحماية الجنائية أحد وأهم أنواع الحماية القانونية بصفة عامة[1]، وتتحقق عن طريق القواعد والنصوص التشريعية التى يُجْرم ويُعاقب بمقتضاها المشرع على المساس بمصالح ذات أهمية، وهذه الأخيرة تشمل فى نطاق الأمن الالكترونى حماية، وتأمين العناصر التالية:-

(أ) تأمين وحماية الشبكة المعلوماتية :

يتباين مفهوم الشبكة المعلوماتية وفقاً للقانون الإماراتي، فقد عرفها أحيانا بأنها ارتباط بين مجموعتين، أو أكثر من البرامج المعلوماتية، ووسائل تقنية المعلومات التى تتيح للمستخدمين الدخول وتبادل المعلومات[2]. وفى أحيان أخرى عرفها المشرع الإماراتى بأنها ارتباط بين أكثر من نظام معلومات، وشبكات الاتصالات، والأنظمة الالكترونية أو أى منها

---

(1) انظر فى هذا الصدد د. عبد الفتاح مصطفى الصيفى : القاعدة الجنائية، دراسة تحليلية لها على ضوء الفقه الجنائى المعاصر، دار النهضة العربية، القاهرة، بدون سنة نشر، ص 3 وما بعدها.

(2) راجع : المادة الأولى من مرسوم بقانون اتحادى رقم (5) لسنة 2012م.

للحصول على البيانات والمعلومات وتبادلها[1]. وهذا التعريف الأخير أوسع نطاقاً حيث يشمل مصطلح الأنظمة الالكترونية.

(ب) تأمين وحماية شبكة الاتصالات :

شبكة الاتصالات هى منظومة تحتوى على جهاز أو وسيلة اتصال أو أكثر، بهدف نقل أو بث أو تحويل أو استقبال أى من خدمات الاتصالات وذلك بواسطة أى طاقة كهربائية أو مغناطيسية أو إلكترومغناطيسية أو إلكتروكيميائية أو إلكتروميكانيكية، وغير ذلك من وسائل الاتصال[2].

(جـ) تأمين وحماية نظم المعلومات :

نظم المعلومات وفقاً للتشريع الإماراتى هى أية وسيلة مادية أو معنوية أو مجموعة وسائل مترابطة أو غير مترابطة تستعمل لتخزين المعلومات وترتيبها وتنظيمها واسترجاعها ومعالجتها وتطويرها وتبادلها، وفقا للأوامر والتعليمات المخزنة بها، ويشمل فى ذلك جميع المدخلات والمخرجات والبنى التحتية المرتبطة بها[3].

(د) تأمين وحماية عمليات جمع المعلومات الالكترونية :

المعلومات الالكترونية وفقا للتشريع الإماراتى لها مدلولان. إحداهما

---

(1) المادة الأولى من مرسوم بقانون اتحادى رقم (3) لسنة 2012م.
(2) المادة الأولى من مرسوم بقانون اتحادى رقم (3) لسنة 2012م.
(3) المادة الأولى من مرسوم بقانون اتحادى رقم (3) لسنة 2012م.

ضيق والأخر يحمل دلالة واسعة. وهـذا الأخـير يشـمل أى معلومـات يمكـن تخزينهـا، ومعالجتها، وتوليدها، ونقلها، بوسائل تقنية المعلومات، وبوجه خاص الكتابة، والصور، والصوت، والأرقام، والحروف، والرموز، والإشارات، وغيرها[1]. أو هى عبارة عن بيانـات ومعلومات ذات خصائص إلكترونية فى شكل نصـوص أو رمـوز أو أصـوات أو رسـوم أو صور أو برامج الحاسب الآلى أو غيرهـا[2].أمـا المعلومـات الالكترونيـة بـالمفهوم الضـيق فهى البيانات التى تمت معالجتها، وأصبح لها دلالـة سـواء كانـت مرئيـة أو صـوتية أو مقروءة[3]. ويؤيد الباحث التعريف الموسع حيث يتضمن مزيـد مـن الحمايـة لمصـالح ذات أهمية بالغة.

ثانياً : منهج المشرع الإماراتى فى تقرير الحماية الفعالة للأمن الالكترونى :

انتهج المشرع الإماراتى فيما يتعلـق بسياسـة الحمايـة للأمـن الالكـتروني، كثـير مـن السبل، وقد كان من أهم هذه السبل، هو إنشـاء الهيئـة الوطنيـة للأمـن الالكـترونى فى دولة الإمارات العربية المتحدة، وسوف نسلط الضوء على هذه الهيئة من خلال النقاط التالية :

---

(1) راجع : المادة الأولى من مرسوم بقانون اتحادى رقم (5) لسنة 2012م.

(2) المـادة رقـم (1) مـن القـانون الاتحـادى رقـم (1) لسـنة 2006 فى شـأن المعـاملات والتجـارة الإلكترونية، فى دولة الإمارات العربية المتحدة.

(3) المادة الأولى من مرسوم بقانون اتحادى رقم (3) لسنة 2012م، بإنشـاء الهيئـة الوطنيـة للأمـن الإلكتروني.

(1) أداة إنشاء الهيئة ومقرها :

أنشئت بموجب أحكام المرسوم بقانون رقم (3) لسنة 2012م، ومقرها الرئيسى مدينة أبوظبي، وهى هيئة عامة تتمتع بالشخصية الاعتبارية، ولها الصلاحيات التنفيذية والرقابية اللازمة وفقا لما حدده هذا المرسوم بقانون، وكذلك واللوائح والقرارات التى تصدر تنفيذا له[1].

(2) أهداف الهيئة واختصاصاتها:

تهدف إلى تنظيم حماية شبكة الاتصالات، ونظم المعلومات، وتطوير وتعديل واستخدام الوسائل اللازمة فى مجال الأمن الالكتروني[2]. ومن أهم اختصاصاتها الفاعلة أيضاً مكافحة جرائم الحاسب الآلي، والشبكة المعلوماتية، وتقنية المعلومات، وإعداد الخطط لمواجهة أية أخطار، أو تهديدات، أو اعتداءات على الأمن الالكتروني[3].

(3) إدارة الهيئة :

يتولى إدارة الهيئة مجلس إدارة يتكون من عدد من الأعضاء لا يزيد على تسعة ولا يقل عن خمسة، ويصدر بتشكيل مجلس الإدارة قرار من رئيس المجلس الأعلى للأمن الوطنى بناء على ترشيح مستشار الأمن الوطني،

---

(1) المادتين (3،2) من مرسوم بقانون اتحادى رقم (3) لسنة 2012م.
(2) المادة (4) من مرسوم بقانون اتحادى رقم (3) لسنة 2012م.
(3) المادة (4) من مرسوم بقانون اتحادى رقم (3) لسنة 2012م.

وتكون مدة العضوية بمجلس الإدارة ثلاث سنوات قابلة للتجديد لمدد مماثلة[1].

(4) الطابع السرى للبيانات والمعلومات المقدمة للهيئة :

وفقاً لنص المادة رقم (10) من المرسوم بقانون اتحادى رقم (3) لسنة 2012، فإنه تعتبر جميع البيانات والمعلومات التى تقدمها الجهات المعنية للهيئة والمتعلقة بمهامها سرية، ولا يجوز للهيئة، أو لأى من العاملين فيها اطلاع أى شخص أو جهة عامة أو خاصة عليها، أو الكشف عنها، أو استخدامها لأى غرض غير تلك التى تحددها اللائحة التنفيذية لهذا المرسوم.

---

(1) المادة (6) من مرسوم بقانون اتحادى رقم (3) لسنة 2012م.

الفصل الثاني

الحماية الجنائية الموضوعية للأمن الالكتروني

تتعلق الحماية الجنائية الموضوعية للأمن الالكتروني، بمجموعة النصـوص القانونيـة التى يحدد بمقتضاها المشرع صور الفعل أو الامتناع عن الفعل المعتبرة جريمـة، والتـى تستوجب عقوبة جنائية. وسوف نعالج ذلك وفق الخطة التالية :

المبحث الأول : الأركان العامة لجرائم الاعتداء على الأمن الالكتروني.

المبحث الثانى : الجزاءات الجنائية المقررة لجرائم الاعتداء على الأمن الالكتروني.

المبحث الأول

الأركان العامة لجرائم الاعتداء على الأمن الالكتروني

تقتضى دراسة الأركان العامة لجرائم الاعتداء على الأمـن الالكـتروني، أن نبحـث فى ماديات هذه الجرائم، وكذلك طبيعة الركن المعنوى فيها، وسوف يكون ذلك من خلال الخطة التالية.

المطلب الأول : الركن المادى فى جرائم الاعتداء على الأمن الالكتروني.

المطلب الثانى : طبيعة الركن المعنوى فى جرائم الاعتداء على الأمن الالكتروني.

المطلب الأول

الركن المادى فى جرائم الاعتداء على الأمن الالكتروني

أولاً : صور السلوك غير المشروع المنشئ للاعتداء على الأمن الالكترونى :

يتحقق الاعتداء على الأمن الالكتروني، وفقا لما للتشريع الإماراتى بأى من صور السلوك غير المشروع الآتية :

- دخول (موقع الكتروني، أو نظام معلومات الكتروني، أو شبكة معلومات، أو وسيلة تقنية معلومات) بدون تصريح، أو بتجاوز حدود التصريح، أو البقاء فيه بصورة غير مشروعة[1].

- دخول (موقع الكتروني، أو نظام معلومات الكتروني، أو شبكة معلومات، أو وسيلة تقنية معلومات) بدون تصريح، أو بتجاوز حدود التصريح، أو البقاء فيه بصورة غير مشروعة، إذا ترتب على ذلك إلغاء، أو حذف، أو تدمير، أو إفشاء، أو إتلاف، أو تغيير، أو نسخ، أو نشر، أو إعادة نشر أى بيانات أو معلومات[2].

- الدخول بدون تصريح إلى (موقع الكتروني، أو نظام معلومات

---

(1) المادة (2-1) مرسوم بقانون اتحادى رقم (5) لسنة 2012 فى شأن مكافحة جرائم تقنية المعلومات.

(2) المادة (2-2) مرسوم بقانون اتحادى رقم (5) لسنة 2012 فى شأن مكافحة جرائم تقنية المعلومات.

الكتروني، أو شبكة معلوماتية، أو وسيلة تقنية معلومات) بقصد الحصول على بيانات حكومية، أو معلومات سرية خاصة بمنشأة مالية، أو تجارية، أو اقتصادية[1]. أو إذا تعرضت هذه البيانات أو المعلومات للإلغاء، أو الحذف، أو الإتلاف، أو التدمير، أو الإفشاء، أو التغيير، أو النسخ أو النشر، أو إعادة النشر[2].

- دخول (موقع الكتروني) بقصد تغيير تصاميمه، أو إلغائه، أو إتلافه، أو تعديله، أو شغل عنوانه[3].

- تزوير (مستند الكتروني) من مستندات الحكومة الاتحادية أو المحلية أو الهيئات أو المؤسسات العامة الاتحادية أو المحلية، أو غيرها[4]. أو استعمال المستند المزور مع العلم بتزويره[5].

- (الحصول أو الاستحواذ أو التعديل أو الإتلاف أو الإفشاء) بغير تصريح لبيانات أى مستند الكتروني، أو معلومات الكترونية، عن طريق الشبكة المعلوماتية أو موقع الكتروني، أو نظام المعلومات الالكتروني، أو وسيلة تقنية معلومات، متعلقة بفحوصات طبية أو تشخيص طبي، أو

---

(1) المادة (4-1) مرسوم بقانون اتحادى رقم (5) لسنة 2012 فى شأن مكافحة جرائم تقنية المعلومات.

(2) المادة (4-2) مرسوم بقانون اتحادى رقم (5) لسنة 2012 فى شأن مكافحة جرائم تقنية المعلومات.

(3) المادة (5) مرسوم بقانون اتحادى رقم (5) لسنة 2012 فى شأن مكافحة جرائم تقنية المعلومات.

(4) المادة (6ـــ1،2) مرسوم بقانون اتحادى رقم (5) لسنة 2012 فى شأن مكافحة جرائم تقنية المعلومات.

(5) المادة (6-3) مرسوم بقانون اتحادى رقم (5) لسنة 2012 فى شأن مكافحة جرائم تقنية المعلومات.

علاج، أو رعاية طبية، أو سجلات طبية[1].

-(إعاقة، أو تعطيل) الوصول إلى شبكة معلوماتية، أو موقع الكتروني، أو نظام معلومات الكتروني[2].

-التحايل على العنوان البروتوكولى للانترنت (باستخدام عنوان وهمي، أو عنوان عائد للغير، أو بأى وسيلة أخري) بقصد ارتكاب جريمة أو الحيلولة دون اكتشافها[3].

- الإدخال العمدى وبدون تصريح (برنامج معلوماتى إلى الشبكة المعلوماتية، أو نظام معلوماتى الكتروني، أو إحدى وسائل تقنية المعلومات) بأن أدى ذلك إلى إيقافها عن العمل، أو تعطيلها أو تدمير أو مسح أو حذف أو إتلاف أو تغيير البرنامج أو النظام أو الموقع الالكترونى أو البيانات أو المعلومات[4]. أو أى فعل عمدى يقصد به إغراق البريد الالكترونى بالرسائل وإيقافه عن العمل أو تعطيله أو إتلاف محتوياته[5].

- استخدام الشبكة المعلوماتية أو نظام معلوماتى الكترونى أو إحدى وسائل تقنية المعلومات، للتوصل بغير حق إلى أرقام أو بيانات بطاقة ائتمانية

---

(1) المادة (7) مرسوم بقانون اتحادى رقم (5) لسنة 2012 فى شأن مكافحة جرائم تقنية المعلومات.

(2) المادة (8) مرسوم بقانون اتحادى رقم (5) لسنة 2012 فى شأن مكافحة جرائم تقنية المعلومات.

(3) المادة (9) مرسوم بقانون اتحادى رقم (5) لسنة 2012 فى شأن مكافحة جرائم تقنية المعلومات.

(4) المادة (10- 1) مرسوم بقانون اتحادى رقم (5) لسنة 2012 فى شأن مكافحة جرائم تقنية المعلومات.

(5) المادة (10- 2) مرسوم بقانون اتحادى رقم (5) لسنة 2012 فى شأن مكافحة جرائم تقنية المعلومات.

أو الكترونية أو أرقام أو بيانـات حسـابات مصرفيـة، أو أى وسـيلة مـن وسـائل الـدفع الالكتروني. أو إذا قصد من ذلك الحصول على أموال الغير، أو الاستفادة مما تتيحه مـن خدمات[1].

- تزوير، أو تقليد، أو نسخ، بطاقة ائتمانية أو بطاقـة مدينـة، أو أى وسـيلة أخـرى من وسائل الدفع الالكـتروني، باسـتخدام إحـدى وسـائل تقنيـة المعلومـات، أو برنـامج معلوماتي. أو قبول التعامل بهذه البطاقات مع العلم بعدم مشروعيتها[2].

- الحصول بدون تصريح على رقم سرى أو شفرة أو كلمة مرور أو أى وسيلة أخرى للدخول إلى وسيلة تقنية معلومات، أو موقع الكتروني، أو نظام معلومـات الكـتروني، أو شبكة معلوماتية، أو معلومات الكترونية. وكذلك كل من (أعد أو صمم أو أنتج أو بـاع أو اشترى أو اسـتورد أو عـرض للبيـع أو أتـاح) أى برنـامج معلومـاتى أو وسـيلة تقنيـة معلومـات، أو روج بـأى طريقـة روابـط لمواقـع الكترونيـة أو برنـامج معلومـاتي، أو أى وسيلة تقنية معلومات مصممة لأغراض ارتكاب أو تسهيل أو التحـريض عـلى ارتكـاب الجـرائم المنصـوص عليهـا فى المرسـوم بقـانون اتحـادى رقـم (5) لسـنة 2012 فى شـأن مكافحة جرائم تقنية المعلومات[3].

(1) المـادة (12) مرسـوم بقـانون اتحـادى رقـم (5) لسـنة 2012 فى شـأن مكافحـة جـرائم تقنيـة المعلومات.
(2) المـادة (13) مرسـوم بقـانون اتحـادى رقـم (5) لسـنة 2012 فى شـأن مكافحـة جـرائم تقنيـة المعلومات.
(3) المـادة (14) مرسـوم بقـانون اتحـادى رقـم (5) لسـنة 2012 فى شـأن مكافحـة جـرائم تقنيـة المعلومات.

- الالتقاط أو الاعتراض العمدى وبدون تصريح لأى اتصال عن طريق أى شبكة معلوماتية، أو إفشاء المعلومات المتحصل عليها عن طريق استلام أو اعتراض الاتصالات بغير وجه حق[1].

- استخدام شبكة معلوماتية، أو نظام معلوماتى الكتروني، أو احدى وسائل تقنية المعلومات، فى الاعتداء على خصوصية شخص فى غير الأحوال المصرح بها قانونا بأن أسترق السمع، أو اعترض، أو سجل أو نقل أو بث أو افشى محادثات أو اتصالات أو مواد صوتية أو مرئية، أو التقط صور للغير، أو نشر أخبار أو مشاهدات أو تعليقات أو بيانات أو معلومات ولو كانت صحيحة وحقيقية[2].

-أى مالك أو مشغل لموقع الكترونى أو شبكة معلوماتية خزن أو أتاح متعمداً أى محتوى غير قانوني، مع علمه بذلك، (أو لم يبادر بإزالة، أو منع الدخول إلى هذا المحتوى) غير القانونى خلال المهلة المحددة فى الإشعار الخطى الموجه له من الجهات المختصة[3].

يتبين من خلال التحديد التشريعى لصور السلوك غير المشروع المنشئ للاعتداء على الأمن الالكتروني، أن أغلبها يتم بسلوك أو فعل ايجابي، ينهى

(1) المادة (15) مرسوم بقانون اتحادى رقم (5) لسنة 2012 فى شأن مكافحة جرائم تقنية المعلومات.
(2) المادة (21) مرسوم بقانون اتحادى رقم (5) لسنة 2012 فى شأن مكافحة جرائم تقنية المعلومات.
(3) المادة (39) مرسوم بقانون اتحادى رقم (5) لسنة 2012 فى شأن مكافحة جرائم تقنية المعلومات.

عنه القانون، ويتمثل فى حركة عضوية إرادية لتحقيق النتيجة التى يعاقب عليها القانون، كإلغاء، أو حذف، أو تدمير، أو إفشاء، أو إتلاف، أو تغيير، أو نسخ، أو نشر، أو إعادة نشر أى بيانات أو معلومات، وغير ذلك من صور الأفعال التى عرضنا لها سلفاً. وقليل جدا من صور هذا السلوك يتطلب فيه المشرع أن يكون بسلوك سلبي، حتى أن الصورة الوحيدة لهذه الجريمة ورد النص على تجريمها إذا تمت بما يسمى بالسلوك السلبى البسيط، أى الإمتناع.

بيد أنه، من المتصور أيضاً فى بعض الحالات، أن يتم الاعتداء على الأمن الالكترونى بأفعال سلبية أو امتناع أعقبته نتيجة ايجابية ناشئة عن هذا الامتناع[1].

ومن ثم يفترض الركن المادى فى هذه الجرائم امتناعا أعقبته نتيجة إجرامية[2]. من ذلك مثلاً إحجام أو امتناع الجهة أو الشخص عن اتخاذ سبل تأمين وحماية الشبكة المعلوماتية، أو شبكة الاتصالات، أو نظم المعلومات، إذا ترتب على ذلك أضرار أو أخطار معينة، تهدد المصالح ذات الأهمية.

---

(1) وهو نوع من الجرائم يتوسط الجرائم الايجابية، والجرائم السلبية. راجع فى هذا الصدد : د. احمد شوقى عمر أبو خطوة : شرح الأحكام العامة لقانون العقوبات، الجزء الأول، النظرية العامة للجريمة، دار النهضة العربية، القاهرة، 1999، ص 172 وما بعدها.

(2) أنظر : د. محمود نجيب حسنى : جرائم الامتناع والمسئولية الجنائية عن الامتناع، دار النهضة العربية، القاهرة،1986، ص 1 وما بعدها.

حيث يلزم لانعقاد المسؤولية عن هذه الأفعال أن يكون هناك واجب أو التزام قـانونى أو تعاقدى على الجهة أو الشخص المسئول، بشأن التـأمين والحمايـة، وأن يكـون لديـه إرادة هذا الامتناع، مع توافر علاقة السببية بين الامتناع والنتيجة المعاقب عليها[1].

وهذه الأفعال الأخيرة، وما يلزم لها من ضوابط لانعقاد المسؤولية عنها، على النحو السالف البيان، لم يهتم المشرع الإماراتى بتجريمها، رغم توافر مقومات الجريمة فيها من حيث خطورتها على الأمن الالكتروني.

ثانياً : طبيعة النتيجة الإجرامية فى جرائم الاعتداء على الأمن الالكترونى :

النتيجة الإجرامية هى الأثر المترتب على السلوك الإجرامـي، وهـى العـدوان الـذى ينال المصلحة أو الحق الذى يقرر له القانون حماية جنائية[2]. وتتميز هذه النتيجـة فى جرائم الاعتداء على الأمن الالكتروني، بمظهرين أساسيين، إحداهما يمثل ضرر بالمصـلحة، والآخر يمثل ثمة خطر، وفيما يلى بيان ذلك :

(أ) النتيجة الإجرامية فى جرائم الاعتداء بالضرر الالكترونى :

توجـد طائفـة مـن جـرائم الاعتـداء عـلى الأمـن الالكـتروني، المنصـوص عليها فى القانون الإماراتي، يتطلب المشرع فى نتيجتهـا الإجراميـة وجـود ضرر

(1) أنظر : د. محمود نجيب حسنى : المرجع السابق، ص 6 وما بعدها.

(2) د. احمد شوقى عمر أبو خطوة : شرح الأحكام العامة لقانون العقوبات، المرجـع السـابق، ص 226.

فعلي، أو تغير مادى فى العالم الخارجي، تدركه الحواس، يصيب المصلحة محل الحماية الجنائية[1]. ولكن رغم ذلك يتميز هذا الضرر بأنه يقترب أحياناً من الضرر المعنوى للمصلحة. من ذلك مثلاً جريمة إلغاء، أو حذف، أو تدمير، أو إتلاف، أو تغيير، موقع الكتروني، أو نظام معلومات الكتروني[2]، أو بيانات حكومية، أو معلومات سرية خاصة بمنشأة مالية، أو تجارية، أو اقتصادية[3]. وهذه الجرائم لا تنعقد فيها المسؤولية وتوقيع العقاب، إلا بتحقق النتيجة الإجرامية التى تطلبها المشرع بالنص القانوني.

(ب) النتيجة الإجرامية فى جرائم تعريض الأمن الالكترونى للخطر :

الغالب فى القانون العام هو تجريم النتائج الضارة، أما تجريم النتائج الخطرة فأمر نادر[4]، وعلى العكس من ذلك تغلب النتائج الخطرة فى كثير من صور جرائم الاعتداء على الأمن الالكتروني. ويميز الفقه الجنائى فى نطاق جرائم الخطر بوجه عام بين نوعين هما (جرائم التعريض للخطر المجرد، وجرائم التعريض للخطر الواقعي)[5].

---

(1) أنظر حول مفهوم النتيجة الإجرامية. د. احمد شوقى عمر أبو خطوه : المرجع السابق، ص 227 وما يليها.

(2) المادة (2-2) مرسوم بقانون اتحادى رقم (5) لسنة 2012 فى شأن مكافحة جرائم تقنية المعلومات.

(3) المادة (4-1) مرسوم بقانون اتحادى رقم (5) لسنة 2012 فى شأن مكافحة جرائم تقنية المعلومات.

(4) د. محمود محمود مصطفى : الجرائم الاقتصادية فى القانون المقارن، الجزء الأول، الأحكام العامة والإجراءات الجنائية، الطبعة الثانية، القاهرة، 1979، ص 105.

(5) راجع فى هذا الصدد: د. أحمد شوقى عمر أبو خطوة : جرائم التعريض للخطر العام، دراسة مقارنة، دار النهضة العربية، القاهرة، 1999، ص29 وما بعدها.

ومن أمثلة جرائم الخطر الواقعي، فى نطاق الاعتداء على الأمن الالكتروني، جريمة الإدخال العمدى وبدون تصريح برنامج معلوماتى إلى الشبكة المعلوماتية، أو نظام معلوماتى الكتروني[1]. وجريمة تزوير (مستند الكتروني) من مستندات الحكومة الاتحادية أو المحلية[2]. وجريمة تزوير، أو تقليد، أو بطاقة ائتمانية، أو أى وسيلة أخرى من وسائل الدفع الالكتروني، باستخدام إحدى وسائل تقنية المعلومات، أو برنامج معلوماتي[3]. وجريمة استخدام الشبكة المعلوماتية، للتوصل بغير حق إلى أرقام أو بيانات بطاقة ائتمانية أو الكترونية أو أرقام أو بيانات حسابات مصرفية[4]. فهذه الجرائم يمثل قدر التغير الذى أحدثته النتيجة قدر واضح نوعاً.

ومن أمثلة جرائم الخطر المجرد فى نطاق الاعتداء على الأمن الالكتروني، جريمة دخول موقع الكتروني، أو نظام معلومات الكتروني، أو شبكة معلومات، بدون تصريح، أو بتجاوز حدود التصريح، أو البقاء فيه بصورة غير مشروعة[5]. فقد نص المشرع الإماراتى صراحة على أن كل من أدخل عمداً وبدون تصريح برنامج معلوماتى إلى الشبكة أو نظام

(1) المادة (10- 1) مرسوم بقانون اتحادى رقم (5) لسنة 2012 فى شأن مكافحة جرائم تقنية المعلومات.

(2) المادة (6-1،2) مرسوم بقانون اتحادى رقم (5) لسنة 2012 فى شأن مكافحة جرائم تقنية المعلومات.

(3) المادة (13) مرسوم بقانون اتحادى رقم (5) لسنة 2012 فى شأن مكافحة جرائم تقنية المعلومات.

(4) المادة (12) مرسوم بقانون اتحادى رقم (5) لسنة 2012 فى شأن مكافحة جرائم تقنية المعلومات.

(5) المادة (2-1) مرسوم بقانون اتحادى رقم (5) لسنة 2012 فى شأن مكافحة جرائم تقنية المعلومات.

معلوماتي، (حتى ولو لم تتحقق النتيجة)، وهى إيقاف أو تعطيل أو حذف أو إتلاف البرنامج أو النظام أو الموقع الالكتروني[1].

وترتيباً على ما سلف ذكره من أمثلة، يتبين أن المشرع الإمارتي لا يعاقب على هذه الجرائم بوصف الشروع، وإنما بوصفها جرائم تامة قائمة بذاتها[2]. والهدف من العقاب على هذه الجرائم وفقا لما لاحظه الفقه الجنائي، هو منع وقوع النتائج الضارة، أو اعتراض سبيل وخطوات السلوك الإجرامى قبل أن يفضى إلى الضرر الفعلى المحقق الوقوع الذى يصيب المصلحة محل الحماية[3]. وهى مرحلة مبكرة ومتقدمة من الحماية.

ثالثاً : علاقة السببية فى جرائم الاعتداء على الأمن الالكترونى :

(أ) صعوبة البحث فى علاقة السببية ودور القاضى فى التثبت منها :

لا يكفى لقيام لتوافر جريمة الاعتداء على الأمن الالكتروني، وانعقاد المسؤولية الجنائية عن نتيجتها سلوك ونتيجة فحسب، بل يلزم وجود علاقة سببية تربط بينهما. ولا يثير البحث فى علاقة السببية على أساس فكرة الضرر، ذات الصعوبات التى نصادفها ونحن بصدد جريمة من جرائم تعريض الأمن الإلكترونى للخطر، ذلك لأنه لم تتحقق بالفعل النتيجة

---

(1) (المادة رقم 10 من القانون 5 لسنة 2012 فى شان مكافحة جرائم تقنية المعلومات).

(2) د. محمود محمود مصطفى : الجرائم الاقتصادية فى القانون المقارن، المرجع السابق، ص 105.

(3) انظر : د. أحمد شوقى عمر أبو خطوة : جرائم التعريض للخطر، المرجع السابق، ص 5 وما بعدها.

الإجرامية حتى يمكن القطع والجزم بفاعلية السلوك فى إحـداثها[1]، وإنما هنـاك فقـط ثمة حالة خطر أو ضرر محتمـل الوقـوع بدرجـة كبـيرة تهـدد المصـالح محـل الحمايـة الجنائية.

ولهذا السبب، يبدو أن الحكم بتوافر الفاعلية السببية بـين السـلوك والنتيجـة فى هذه الجرائم، تقوم على الاحتمال التقديرى والسابق على وقـوع النتيجـة، متـى كـان من الممكن تقييم النشاط بأنه يملك مقومات وقوع النتيجة المحتملة[2]. وهى بالطبع سببية كامنة، يتم التوصل إليهـا وتقـدير توافرهـا عـلى الافـتراض المنطقـي، ذلـك لأن سلوك الفاعل لم يتولد عنة نتيجة مادية فى العالم الخارجي. ومـن ثـم، فـإن المحكمـة تستخلص قيام رابطة السببية من الاحتمال القاطع بفاعلية وصلاحية السـلوك القـائم فى إحداث النتيجة التى لم تتحقق. بعكس ذلك فى نطاق المسؤولية على أسـاس فكـرة الضرر الـذى تحقـق بالفعـل، فـإن المحكمـة تـرتكن فى حكمهـا عـلى تـوافر رابطـة السببية على الواقع والمستفاد مـن كـون النتيجـة التـى تحققـت وترتبـت فعـلاً عـلى

(1) د. مأمون محمد سلامة: قانون العقوبات، القسـم العـام، الطبعـة الثالثـة، دار الفكـر العـربي، القاهرة، 1990، ص 169.

(2) د. مزهر جعفر عبد السلام : جريمة الامتناع، الطبعة الأولى، الإصـدار الأول، دار الثقافـة للـنشر والتوزيع، عمان، الأردن، 1999، ص 113، د. عبد المنعم محمد إبراهيم رضوان : موضـع الضرر فى البنيان القانونى للجريمة، دراسة تحليلية تأصـيلية، رسـالة دكتـوراه، كليـة الحقـوق، جامعـة القاهرة، 1994، ص196.

السلوك المرتكب، وهو الضرر الناشئ عن العمل أو السلوك الإجرامي[1].

(ب) تناسب نظرية السببية الملائمة مع جرائم تعريض الأمن الالكترونى للخطر:

الواقع أنه يبدو أن الإسناد الموضوعى لنظام المسؤولية الجنائية فى نطاق الاعتداء على الأمن الالكترونى على أساس فكرة (الضرر أو الخطر) يتلاءم مع نظرية السببية الملائمة[2]. ذلك لأن الحكم بتوافر الفاعلية السببية خصوصاً فى مجال المسؤولية على أساس الخطر، يقوم على الاحتمال باعتبار أن النتيجة لم تتحقق فعلاً حتى يمكن القطع والجزم بفاعلية السلوك فى إحداثها[3].

---

(1) د. مأمون محمد سلامة : قانون العقوبات، القسم العام، دار النهضة العربية، القاهرة، 1996، ص 168 وما بعدها ؛ د. عبد المنعم محمد إبراهيم رضوان : المرجع السابق، ص 183 وما بعدها.

(2) ومؤدى نظرية السببية الملائمة أن النتيجة الإجرامية فى صورتها الواقعية المحددة هى ثمرة لجميع العوامل التى أسهمت فى إحداثها، وأن السلوك الإجرامى لا يعتبر سبباً لوقوع النتيجة إلا إذا تبين انه صالح إلى إحداثها وفقا للمجرى العادى للأمور، فيعد سلوك الجانى سبباً فى النتيجة ولو ساهمت معه فى إحداثها عوامل أخرى سابقة عليه أو معاصرة معه أو لاحقه له، ما دامت هذه العوامل متوقعة ومألوفة، فتكون النتيجة متوقعة وفقا للمجرى العادى للأمور إذا كانت مألوفة وليست بسبب تدخل عوامل شاذة أو غير مألوفة.

د. محمود نجيب حسنى : علاقة السببية، دار النهضة العربية، القاهرة، 1984، ص 160 ؛ د. أحمد شوقى أبو خطوة : المرجع السابق، ص234 وما بعدها.

(3) د. مأمون محمد سلامة: المرجع السابق، ص168؛ د. أحمد شوقى عمر أبو خطوة: جرائم التعريض للخطر العام، المرجع السابق، ص44.

ونشير هنا، إلى أن نظرية السببية الملائمة حلت محل النظرية التقليدية، وهى نظرية تعادل الأسباب، وهذه الأخيرة تقوم على الحكم اللاحق على تحقيق النتيجة المادية وهو ما لا يتلاءم أبداً وعلى الأقل مع انعقاد المسؤولية على أساس فكرة الخطر أو الضرر المحتمل[1].

وواقع الأمر، أنه بتطبيق معيار السببية الملائمة على المسؤولية الجنائية على أساس فكرة الخطر، يعنى توافر الخطر إذا كان السلوك الذى باشره الجانى قد سبقته أو عاصرته ظروف أو عوامل تجعل من المحتمل وفقاً للسير العادى للأمور وقوع النتيجة، وهى تعريض المصالح لضرر محتمل الوقوع[2].

ومن ثم، يتعين على قاضى الموضوع التثبت من توافر علاقة السببية كعنصر هام فى المسؤولية على أساس الضرر المحتمل، أو الخطر الفعلي، بنفس الأساس الذى يرتكن إليه فى إثباتها بين السلوك والنتيجة فى نطاق الضرر الذى تحقق وقوعه فعلاً.

ويعتمد هذا الإثبات على افتراضات منطقية، ولكنها غير مؤكدة، مؤداها أن السلوك الايجابى أو السلبى الذى ارتكب، من شأنه تعريض المصلحة محل الحماية الجنائية لخطر الإضرار بها[3].

---

(1)د. أحمد شوقى عمر أبو خطوة : المرجع السابق، ص 44.

(2) د. مأمون محمد سلامة : المرجع السابق، ص169.

(3) د. عبد المنعم محمد إبراهيم رضوان : المرجع السابق، ص 183.

وفى هذا الصدد يرى جانب كبير من الفقه[1]، ويؤيده جانب كبير من القضاء[2]، أن المعيار المعول عليه لقياس التوقع أو الاحتمال والذى تبنى على أساسه صفة الخطورة بصفة عامة، هو معيار (موضوعى وليس شخصي). بمعنى أنه لا ينظر إلى موقف الجانب النفسى لمرتكب الفعل غير المشروع حيال هذا التوقع أو الاحتمال وهل هو توقع فعلاً من عدمه، وإنما يستند معيار هذا التوقع والاحتمال على معيار موضوعي، مناطه الفعل أو الخطأ ذاته.

(1) من هذا الرأى : د. مأمون محمد سلامة : المرجع السابق، ص 169؛ د. محمود نجيب حسنى : علاقة السببية، المرجع السابق، ص 161 وما بعدها؛ د. أحمد شوقى عمر أبو خطوة: جرائم التعريض للخطر العام، المرجع السابق، ص 45.

(2)راجع أحكام القضاء فى تأييد المذهب الموضوعى – نقض 8 ابريل سنة 1974 - مجموعة أحكام النقض- س 25، ص 395 ونقض 3 يناير 1980- مجموعة أحكام النقض- س31، ص 21.

المطلب الثاني

طبيعة الركن المعنوى فى جرائم الاعتداء

على الأمن الالكتروني

يقوم الركن المعنوى للجريمة بصفة عامة على الخطأ، وينقسم الخطأ فى النظرية العامة للركن المعنوى للجريمة إلى نوعين هما : (الخطأ العمدي، والخطأ غير العمدي)، وسوف نعالج ذلك فى نطاق جرائم الاعتداء على الأمن الالكتروني.

أولاً : المعالجة التشريعية للخطأ العمدى فى جرائم الاعتداء على الأمن الالكتروني:

(أ) تطلب العمد أو القصد الجنائى صراحة :

حدد المشرع الإماراتى بموجب بعض النصوص القانونية التى تحمى من مظاهر الاعتداء على الأمن الالكترونى صورة الركن المعنوى صراحة، بأن تطلب العمد صراحة لقيام هذه الجريمة. من ذلك مثلاً جريمة الإدخال العمدى لبرنامج معلوماتى إلى الشبكة المعلوماتية، أو نظام معلوماتى الكتروني، أو إحدى وسائل تقنية المعلومات[1]. أو أى فعل عمدى يقصد به إغراق البريد الالكترونى بالرسائل وإيقافه عن العمل أو تعطيله أو إتلاف

(1) المادة (10- 1) مرسوم بقانون اتحادى رقم (5) لسنة 2012 فى شأن مكافحة جرائم تقنية المعلومات.

محتوياته[1]، وكذلك جريمة الالتقاط أو الاعتراض العمدى وبدون تصريح لأى اتصال عن طريق أى شبكة معلوماتية[2]. ومن ثم، يجب الالتزام بهذا التحديد التشريعى لصورة الخطأ المتطلبة لقيام الجريمة.

(ب) تطلب القصد الجنائى أو العمد بطريق غير مباشر :

توجد طائفة من الجرائم الواردة بالمنظومة التشريعية لحماية الأمن الالكترونى فى التشريع الإماراتي، يستفاد منها أن المشرع يتطلب القصد الجنائى كركن معنوى فى هذه الجرائم بطريق غير مباشر، من خلال الألفاظ والمصطلحات الواردة بالنص التجريمي، كأن يتطلب المشرع أن تقع الجريمة مثلاً بسوء نية، أو بطريق الغش، أو اشتراط علم الجاني.

من ذلك مثلاً جريمة الدخول بدون تصريح إلى نظام معلومات الكتروني، بقصد الحصول على بيانات حكومية، أو معلومات سرية خاصة بمنشأة مالية، أو تجارية، أو اقتصادية[3]. وجريمة دخول (موقع الكتروني) بقصد أو إلغائه، أو إتلافه[4]. أو جريمة التحايل على العنوان البروتوكولى للانترنت بقصد ارتكاب جريمة أو الحيلولة دون اكتشافها[5]. ومن أمثلة

(1) المادة (10- 2) مرسوم بقانون اتحادى رقم (5) لسنة 2012 فى شأن مكافحة جرائم تقنية المعلومات.

(2) المادة (15) مرسوم بقانون اتحادى رقم (5) لسنة 2012 فى شأن مكافحة جرائم تقنية المعلومات.

(3) المادة (4-1) مرسوم بقانون اتحادى رقم (5) لسنة 2012 فى شأن مكافحة جرائم تقنية المعلومات.

(4) المادة (5) مرسوم بقانون اتحادى رقم (5) لسنة 2012 فى شأن مكافحة جرائم تقنية المعلومات.

(5) المادة (9) مرسوم بقانون اتحادى رقم (5) لسنة 2012 فى شأن مكافحة جرائم تقنية المعلومات.

هذه الجرائم فى التشريع الفرنسي، جريمة الدخول إلى نظام الكتروني، ثم البقاء فيه بطريق الغش[1]. وهذه العبارات تدل بطبيعتها على تطلب القصد الجنائي.

(جـ) القصد الخاص فى جرائم الاعتداء على الأمن الالكترونى :

توجد طائفة من الجرائم الواردة بالمرسوم بقانون اتحادى رقم (5) لسنة 2012 فى شأن مكافحة جرائم تقنية المعلومات، يتطلب المشرع الإماراتى فيها قصد خاص يقوم على أساس غاية معينة أو مسار بعيد تسلكه إرادة الجانى أبعد مما هو عليه فى القصد العام القائم بالطبع على عنصرى (الإرادة والعلم). من ذلك مثلاً جريمة التحايل على العنوان البروتوكولى للانترنت باستخدام عنوان وهمي، أو عنوان عائد للغير بقصد ارتكاب جريمة أو الحيلولة دون اكتشافها[2]. وجريمة الدخول بدون تصريح إلى شبكة معلوماتية بقصد الحصول على بيانات حكومية، أو معلومات سرية خاصة بمنشأة مالية، أو تجارية، أو اقتصادية[3]. وجريمة دخول موقع الكترونى بقصد تغيير تصاميمه، أو إلغائه، أو إتلافه، أو تعديله، أو شغل عنوانه[4].

---

(1) المادة رقم (323-1) من قانون العقوبات الفرنسي، المعدلة بموجب القانون رقم (575 لسنة 2004).

Article 323-1 Modifié par Loi n°2004-575 du 21 juin 2004 - art. 45 JORF 22 juin 2004

(2) المادة (9) مرسوم بقانون اتحادى رقم (5) لسنة 2012 فى شأن مكافحة جرائم تقنية المعلومات.

(3) المادة (4-1) مرسوم بقانون اتحادى رقم (5) لسنة 2012 فى شأن مكافحة جرائم تقنية المعلومات.

(4) المادة (5) مرسوم بقانون اتحادى رقم (5) لسنة 2012 فى شأن مكافحة جرائم تقنية المعلومات.

وترتيبا على ما سلف، فإن القصد الخاص المتطلب فى الجرائم السالفة البيان يلعب دوراً هاماً لاكتمال البنيان القانونى للجريمـة، ومـن ثـم ينهـار هـذا البنيـان بتخلفـه ولا يتبقى شئ يسأل عنه الجاني، كما لو تخلفت لديه نية الإلغاء، أو الإتـلاف، أو التعـديل، فى جريمة دخول موقع الكترونى أو نظام معلوماتى فى الأمثلة السالفة البيان.

ثانياً : جرائم الاعتداء على الأمن الالكترونى فى نطاق الخطأ غير العمدى :

(أ) اتجاهات السياسة الجنائية الحديثة :

يعتبر الخطأ العمدى الصورة الثانية للركن المعنوى فى الجريمة، وفى هذا النوع مـن الخطأ تتجه إرادة الفاعل إلى العمل أو الامتنـاع دون نتائجـه، ويكمـن الخطـأ فى هـذه الصورة فى أن الفاعل لم يتخذ نتائج فعله فى اعتباره[1]. أى أن مقدار سيطرة الجانى على ماديات الجريمة غير العمدية يكون أقل قدراً منه فى الجرائم العمدية[2].

وعـلى ضـوء مـا سـلف، فـإن السياسـة الجنائيـة الحديثـة تتجـه إلى تجـريم الاعتـداء غـير العمـدى عـلى المصـالح محـل الحمايـة الجنائيـة فى نطـاق الأنظمـة

---

(1) أنظر : د. عبد العظيم مرسى وزير : شرح قانون العقوبات، القسم العام، الجزء الأول، النظرية العامة للجريمة، الطبعة الرابعة، دار النهضة العربية، القاهرة، 2006، ص 362 وما يليها.

(2) أنظر : د. محمود نجيب حسنى : النظرية العامة للقصد الجنائي، دراسة تأصيلية مقارنة للركن المعنوى فى الجرائم العمدية، الطبعة الثالثة، دار النهضة العربية، القاهرة، 1988، ص 11.

الالكترونية. ولعل السبب فى ذلك أن هناك بعض الحالات التى يدخل فيها مرتكب الفعل إلى الأنظمة المعلوماتية قد تكون بغرض الترفيه، ومع ذلك قد ينتج عنها أضراراً خطيرة تلحق بأنظمة المعلومات وخصوصاً ما يتعلق منها بالأمن القومي، أو مصلحة الدولة الاقتصادية، أو علاقاتها الدولية والإقليمية، رغم أن نية الجانى فيها لا تتجه إلى الإتلاف أو إعاقة النظام.

(1) موقف المشرع الأمريكى :

اتجه المشرع الأمريكى نحو سياسة تجريم الاعتداء غير العمدى فى نطاق بيئة النظم الالكترونية. وقد كان الدافع وراء ذلك قضية " موريتس" حيث تسبب هذا الأخير فى إعاقة عدد كبير من أنظمة الحاسبات نتيجة إدخاله برنامجاً خبيثا إلى شبكة المعلومات، دون أن تتجه نيته إلى إحداث النتيجة، وقد تحملت الحكومة الأمريكية عدة ملايين من الدولارات لإعادة تشغيل هذه الأنظمة[1].

لذلك فقد راعى المشرع الأمريكى هذا الأمر حين قيامه بالتعديلات التشريعية للقانون الفيدرالى لجرائم الحاسبات الآلية فى سنة 1996. فقد ميز المشرع الأمريكى بموجب المادة رقم (1030/أ) من القانون المشار إليه بين الدخول المصرح به والتى تكون الجريمة غير عمدية فى هذه الحالة،

(1) أنظر : د. نائله عادل محمد فريد قورة : جرائم الحاسب الاقتصادية، دراسة نظرية تطبيقية، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، 2013، ص 229.

والدخول المصرح به إلى نظام الحاسب وفيها تكون الجريمة غير عمدية.

وقد جاء بمضمون تقرير مجلس الشيوخ الأمريكى عام 1996 بخصوص تعديل المواد الخاصة بجرائم الحاسبات الآلية، بأن الدخول غير المصرح به إلى نظام الحاسب الآلى هو سلوك غير مشروع فى ذاته، ويجب أن تتقرر المسئولية لمرتكبه عن الإتلاف الذى يلحق بالمعلومات أو النظام نتيجة لهذا الدخول سواء اتجهت نية محدثة إلى تحقيقه أو حدث نتيجة خطأ[1].

(2) موقف المشرع الفرنسى :

انتهج المشرع الفرنسى ذات المسار الذى انتهجه المشرع الأمريكي، من حيث تجريم الاعتداء غير العمدى على الأنظمة الالكترونية. فقد نص بمقتضى المادة رقم (323-1) من قانون العقوبات الجديد على تعديل ومحو البيانات، حتى ولو تم ذلك عن طريق الخطأ، أى دون توافر قصد التغيير أو الحذف، ويفترض ذلك فى جريمة التداخل أو البقاء فى نظام الكترونى بطريق الغش[2].

كما يعاقب أيضا بذات المادة على الإتلاف غير العمدى للمعلومات إذا كان الدخول إلى النظام أو البقاء فيه غير مصرح به (المادة 323 عقوبات

---

(1) Senate Report No 104-357 . 104 th Congress , 2 nd Session Detailed discussion of The NII Protection Act (1996).

(2) أنظر : د. غنام محمد غنام : دور قانون العقوبات فى مكافحة جرائم الكمبيوتر، المرجع السابق، ص 153.

فرنسى المعدلة بموجب القانون الصادر سنة 2004)[1]. ومن ناحية أخرى، يشدد المشرع الفرنسى العقاب إذا ترتب على الدخول غير المصرح محو أو تعديل للمعلومات أو إفساده. والجدير بالإشارة إليه أن الخطأ غير العمدى ينصرف إلى إتلاف المعلومات، أما الدخول والبقاء غير المصرح به داخل النظام يجب أن يكون عمدياً.

(3) موقف المشرع الإماراتي:

إن الملاحظ على المشرع الإماراتى انه لم ينص صراحة على تطلب الخطأ غير العمدى لإمكان تحقق الركن المعنوى فى جرائم الاعتداء على الأمن الالكتروني، فالصور الواردة للركن المعنوى فى هذه الطائفة من الجرائم لا تخرج عن ثلاث افتراضات. (الأول) إما أن يتطلب المشرع العمد صراحة، و(الثاني) أن يتطلب العمد بطريق غير مباشر، و(الثالث) أن يسكت المشرع عن بيان صورة معينة للركن المعنوى فى هذه الجرائم. وإزاء هذا الموقف فإن الفقه الجنائى فى التشريعات التى تتشابه مع موقف المشرع الإماراتي، تتجه

(1) Article 323-1 Modifié par Loi n°2004-575 du 21 juin 2004 - art. 45 JORF 22 juin 2004 Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30000 euros d'amende. Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 45000 euros d'amende.

إلى تفسير ذلك على نحو ثلاث نظريات أساسية[1]:-

النظرية الأولى : ترى أن يكون قصد الشارع المساواة بين الخطأ العمدى والخطأ غير العمدى، فى إمكان تحقق الجريمة بأى منهم فتقع الجريمة بمجرد وقوع المخالفة، سواء تعمد الجانى المخالفة، أو وقعت بسبب إهماله أو عدم احتياطه[2].

النظرية الثانية : ترى ضرورة الرجوع إلى الأصل العام فى التجريم، الذى يعتبر عدم النص على نوع القصد يمثل العمد ولا عقاب على الإهمال إلا بنص صريح[3]. إلا فى مواد المخالفات التى يستوى فيها العمد مع الخطأ.

النظرية الثالثة : ترى أن تكون هذه الجرائم من قبيل الجرائم المادية، التى

---

(1) أنظر فى بيان ذلك : د. عبد الرءوف مهدى : المسئولية الجنائية عن الجرائم الاقتصادية، فى القانون المقارن، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، 1974، ص 168، بند رقم (99). وأنظر أيضاً : د. غنام محمد غنام : الحماية الجنائية للادخار فى شركات المساهمة، دار النهضة العربية، القاهرة، 1988، ص 84 وما بعدها.

(2) أنظر : د. محمود محمود مصطفى : الجرائم الاقتصادية فى القانون المقارن، المرجع السابق، ص 116؛ د. غنام محمد غنام : المرجع السابق، ص 85.

(3) أنظر : د. عبد الرءوف مهدى : المسئولية الجنائية عن الجرائم الاقتصادية، المرجع السابق، ص 193، د. أحمد شوقى عمر أبو خطوه : المرجع السابق، ص 342، د. محمود كبيش : المسئولية الجنائية لمراقب الحسابات فى شركات المساهمة، دراسات مقارنة فى القانونين المصرى والفرنسي، دار النهضة العربية، القاهرة، 1992، ص 75 وما بعدها .

A. Vitu " La protection penal de l'interet public et l'interet des associes dans les societes commerciales et civiles " Rapport presente aux cinquieme journees juridiques Franco-Italienne, Paris , Nancy , 5 – 10 juin 1967.

يستهدف المشرع من خلالها تحقيق أغراض تنظيمية يراها ضرورية لتنظيم المجتمع[1]، ومن أجل ذلك لا يتطلب المشرع إثبات العمد أو عدم الحيطة، ويكتفى بمجرد وقوع الفعل المادى الذى يعد دليلاً على خطأ الجاني، ومن ثم لا يحتاج إثبات عنصر الخطأ فى جانب الجاني[2].

والنتيجة العملية للمساواة بين العمد والخطأ، على النحو السالف البيان، وفقاً لما قرره بعض الفقه الجنائي، هو أنه لا يصح التمسك بالجهل بأحكام هذه القوانين، فى الجرائم التى يعاقب فيها على مخالفة أحكام هذا القانون[3].

ثانياً : الاتجاهات التشريعية الحديثة نحو وضع قاعدة عامة لتحديد نوع الخطأ :

لم تضع اغلب القوانين العقابية فى التشريعات المقارنة خصوصا التشريعات القديمة، نصوصاً تقرر قاعدة يرجع إليها فى حالة عدم بيان صورة الركن المعنوى فى نص التجريم[4].

إلا أن الملاحظ على اغلب المدونات العقابية الحديثة بدأت تتخذ

(1) أنظر : د. مصطفى كامل كيره : الجرائم الاقتصادية، دار النهضة العربية، 1983، ص 171 .

(2) أنظر : د. حسنى أحمد الجندى : القانون الجنائى للمعاملات التجارية، الكتاب الأول، القانون الجنائى للشركات، دار النهضة العربية، القاهرة، 1989، ص151 .

(3) أنظر فى بيان ذلك بالتطبيق على أحكام قانون الشركات. د. غنام محمد غنام : المرجع السابق، ص 85.

(4) د. عبد الرءوف مهدى : شرح القواعد العامة لقانون العقوبات، القاهرة، 2004، ص 445.

مسارها نحو وضع قاعدة عامة بشأن الحالات التى يسكت فيها المشرع عن التصريح بصورة الركن المعنوى الذى يتطلبه لانعقاد الجريمة.

من ذلك مثلاً قانون العقوبات الفرنسى الجديد المعمول به فى مارس 1994، حيث نص بموجب المادة رقم (121 -3) المعدلة بالقانون رقم (647- لسنة 2000) على أنه " لا جناية ولا جنحة بدون توافر قصد ارتكابها"[1]. وبذلك لا يعاقب المشرع على عدم الاحتياط أو الإهمال إلا بنص خاص فى القانون[2].

وفى ذات الاتجاه سار المشرع الايطالى بموجب المادة رقم (42) من قانون العقوبات الايطالى التى تنص على أنه " لا عقاب على فعل يعد فى القانون جريمة، ما لم يكن قد ارتكب عمدا، عدا حالات الجريمة المتعدية، أو جريمة الخطأ التى يعينها القانون صراحة[3] ".

---

(1) Article 121-3 - Modifié par Loi n°2000-647 du 10 juillet 2000 - art. 1 JORF 11 juillet 2000 . "Il n'y a point de crime ou de délit sans intention de le commettre".

(2) د. شريف سيد كامل : تعليق على قانون العقوبات الفرنسى الجديد، القسم العام، الطبعة الأولي، دار النهضة العربية، القاهرة، 1998، ص 90، بند (50).

(3) Art. 42. Responsabilità per dolo o per colpa o per delitto preterintenzionale. Responsabilità obiettiva. Nessuno può essere punito per un'azione od omissione preveduta dalla legge come reato, se non l'ha commessa con coscienza e volontà. Nessuno può essere punito per un fatto preveduto dalla legge come delitto, se non l'ha commesso con dolo, salvi i casi di delitto preterintenzionale o colposo espressamente preveduti dalla legge. La legge determina i casi nei quali l'evento è posto altrimenti a carico dell'agente, come conseguenza della sua azione od omissione. Nelle contravvenzioni ciascuno risponde della propria azione od omissione cosciente e volontaria sia essa dolosa o colposa.

المبحث الثاني

الجزاءات الجنائية المقررة لجرائم

الاعتداء على الأمن الالكتروني

الجزاء هو أثر حتمى لكل جريمة[1]، وتدور أهدافه حول ثلاثة محاور أساسية هى : الزجر، والعدالة، والإصلاح[2]. ولهذا يعرف الفقه الجنائى العقوبة بأنها المظهر القانونى لرد الفعل الاجتماعى إزاء الجناة[3]، وتتنوع الجزاءات المنصوص عليها وفقاً للقواعد القانونية التى تحمى الأمن الالكتروني، فى التشريع الإماراتي، وسوف نعالج ذلك على نحو الخطة التالية.

المطلب الأول: منهج اختيار الجزاءات المقررة لجرائم الاعتداء على الأمن الالكتروني.

المطلب الثانى : تقييم خطة المشرع الإماراتى فى تقرير الجزاءات.

---

(1) د. محمد عيد الغريب : شرح قانون العقوبات القسم العام، النظرية العامة للعقوبة والتدابير الاحترازية، بدون دار نشر، القاهرة، 1999-2000، ص961.

(2) Rotman " L'evolutuion de la pense juridique sur le but de la sanction penale " Melange Ancel , 1975 , 11. p. 163.

(3) د. أحمد عوض بلال : محاضرات فى الجزاء الجنائي، دار النهضة العربية، القاهرة، 2000 – 2001،ص 6.

المطلب الأول

منهج اختيار الجزاءات المقررة لجرائم الاعتداء على الأمن الالكتروني

أولا: صور الجزاءات المقررة لجرائم الاعتداء على الأمن الالكترونى :

انتهج المشرع الإماراتى فكرة التنوع فى العقوبات، تبعاً لجسامة الجريمة فى مجال الاعتداء على الأمن الالكتروني، وتتمثل مظاهر هذا التنوع فى تقرير الجزاءات التالية:

(1) عقوبة السجن المؤقت والغرامة :

انتهج المشرع الإماراتى عقوبة السجن المؤقت والغرامة معاً كجزاء جنائى لبعض صور الاعتداء الشديد على الأمن الالكتروني. من ذلك تقرير عقوبة السجن المؤقت والغرامة التى لا تقل عن مائتين وخمسين ألف درهم، ولا تجاوز مليون وخمسمائة ألف درهم، لكل من دخل بدون تصريح إلى موقع الكتروني، أو شبكة معلوماتية، بقصد الحصول على بيانات حكومية، أو معلومات سرية خاصة بمنشأة مالية، أو تجارية، أو اقتصادية. إلا أن المشرع رفع الحد الأدنى للعقوبة فى هذه الجرائم لعقوبة السجن بحيث لا تقل عن خمس سنوات، والغرامة التى لا تقل عن (500,000) ألف درهم ولا تجاوز (2) مليون درهم، أذا تعرضت هذه البيانات للإلغاء أو الحذف

أو الإتلاف أو التدمير[1].

أضف إلى ذلك فقد انتهج المشرع الإماراتى عقوبة السجن المؤقت وحدها، دون الغرامة، لكل من حصل أو استحوذ أو أتلف بغير تصريح بيانات مستند الكترونى أو معلومات الكترونية، وكانت هذه البيانات تتعلق بفحوصات أو تشخيص طبي[2].

كما قيد المشرع الإماراتى أحياناً الحد الأدنى لعقوبة السجن بمدة لا تقل عن خمس سنوات والغرامة التى لا تقل عن خمسمائة ألف درهم ولا تجاوز ثلاثة ملايين درهم، أو بإحدى هاتين العقوبتين، لكل من أدخل عمداً وبدون تصريح برنامج معلوماتى إلى الشبكة المعلوماتية، بأن أدى ذلك إلى إيقافها عن العمل أو تعطيلها[3].

(2) عقوبة الحبس والغرامة :

انتهج المشرع الإماراتى عقوبة الحبس والغرامة معاً أو إحداهما، فى أغلب صور جرائم الاعتداء على الأمن الالكتروني، وقد انتهج مبدأ التنوع فى مدة الحبس، وكذلك فى مقدار الغرامة. من ذلك مثلاً ما تنص عليه المادة رقم (2-1) من قانون مكافحة جرائم تقنية المعلومات التى يعاقب

(1) المادة (4) من مرسوم بقانون اتحادى رقم (5) لسنة 2012م، فى شأن مكافحة جرائم تقنية المعلومات.

(2) المادة (7) من مرسوم بقانون اتحادى رقم (5) لسنة 2012م، فى شأن مكافحة جرائم تقنية المعلومات.

(3) المادة (10) من مرسوم بقانون اتحادى رقم (5) لسنة 2012م، فى شأن مكافحة جرائم تقنية المعلومات.

بمقتضاها بالحبس والغرامة التى لا تقل عن مائة ألف درهـم، ولا تزيـد عـلى ثلاثمائـة ألف درهم، أو بإحدى هاتين العقوبتين، لكل من دخل موقع الكـترونى بـدون تصريـح، أو البقاء فيه بصورة غير مشروعة.

ومن ناحية أخري، اتجه المشرع الإماراتى نحو تقييد الحـد الأدنى لعقوبـة الحـبس، بحيث لا تقل عن ستة أشهر والغرامة التى لا تقل عن مائة وخمسـين ألـف درهـم ولا تجاوز سبعمائة وخمسون ألـف درهـم، أو بإحـدى هـاتين العقـوبتين، إذا ترتـب عـلى دخول شبكة معلومات بدون تصريح، إلغاء أو حـذف أو تـدمير أو إفشـاء للبيانـات أو المعلومات[1].

(3) الظروف المشددة للعقوبة :

يعد ظرفاً مشددا للعقوبة المقررة لجرائم الاعتداء على الأمن الالكـتروني، وفقـا لمـا نصت عليه المادة رقم (46-2) من مرسوم بقـانون اتحـادى رقـم (5) لسـنة 2012م، فى شأن مكافحة جرائم تقنية المعلومات، ارتكاب أى جريمة منصوص عليهـا بموجـب هـذا المرسـوم، لحسـاب أو لمصـلحة دولـة أجنبيـة، أو أى جماعـة إرهابيـة، أو مجموعـة أو جمعية أو منظمة أو هيئة غير مشروعة. كما لا يخل تطبيق العقوبات المنصوص عليها فى هذا المرسوم بقانون، بأى عقوبة أشد ينص عليهـا أيضـاً فى قـانون العقوبـات، أو أى قانون آخر[2].

---

(1) المادة (2-2) من مرسوم بقانون اتحادى رقم (5) لسنة 2012م، فى شأن مكافحة جـرائم تقنيـة المعلومات.

(2) المادة (48) من مرسوم بقانون اتحادى رقم (5) لسنة 2012م، فى شأن مكافحـة جـرائم تقنيـة المعلومات.

والجدير بالإشارة إليه أنه يعتبر ظرفاً مشدداً وفقاً (للقانون الانجليـزي)، فى جريمـة الدخول إلى نظام الكتروني، أو معلوماتي، إذا كانت نية الفاعل تتجه إلى ارتكـاب جريمـة أخرى أشد من جريمة التدخل، حتى ولو لم تقع هذه الجريمـة الأشـد، أو كانـت جريمـة مستحيلة[1]. كما يعتبر ظرفاً مشددا لهذه الجريمة فى (القانون الفرنسي) إذا ترتـب عـلى ذلك إلغاء، أو تعديل، بيانات مبرمجة فى النظام، أو الإخلال بسير النظام[2].

(4) حالات تخفيف العقوبة أو الإعفاء منها :

وفقاً لنص المادة رقم (45) من مرسـوم بقـانون اتحـادى رقـم (5) لسـنة 2012 فى شأن مكافحة جرائم تقنية المعلومات، تـقضى المحكمـة، بنـاء عـلى طلـب مـن النائـب العام، بتخفيف العقوبة أو بالإعفاء منها، عمن أدلى من الجناة إلى السلطات القضـائية أو الإدارية بمعلومات تتعلق بأى جريمة من الجرائم المتعلقة بأمن الدولة وفقاً لأحكـام هذا المرسوم بقـانون، متـى أدى ذلـك إلى الكشـف عـن الجريمـة ومرتكبيهـا أو إثباتهـا عليهم، أو القبض على أحدهم.

---

(1) Maris Cremona, Jonathan Herring MA, Criminal law, Macmilan, 1998, p.235.

(2) المادة رقم (323-1) من قانون العقوبات الفرنسى المعدلة بموجب القانون رقم (575 /2004).

(5) العقاب على الشروع :

نص المشرع الإماراتى بموجب المادة رقم (40) من مرسوم بقانون اتحادى رقـم (5) لسنة 2012 فى شأن مكافحة جرائم تقنية المعلومات، عـلى أنـه " يعاقـب عـلى الشروع فى الجنح المنصوص عليها فى هذا المرسوم بنصف العقوبة المقررة للجريمة التامة".

(6) المصـــادرة :

نص المشرع الإماراتى بموجب المادة (41) من مرسوم بقانون اتحادى رقم (5) لسنة 2012 فى شأن مكافحة جرائم تقنية المعلومـات، عـلى عقوبـة المصـادرة، كتـدبير عينـى وقائى على الأشياء والأدوات التى استعملت فى ارتكاب الجريمة، أو كانت محلاً للجريمـة الجريمة، أو الأشياء المضبوطة. وقد جاء بهذه المادة السالفة البيان أنه مع عدم الإخلال بحقوق الغير حسنى النيـة يحكـم فى جميـع الأحـوال بمصـادرة الأجهـزة أو الـبرامج أو الوسائل المستخدمة فى ارتكاب أى من الجرائم المنصوص عليها فى هذا المرسوم بقـانون أو الأموال المتحصلة منها، أو بمحو المعلومات أو البيانات أو إعدامها.

(7) الغـلق الكلى أو المؤقت :

غلق المنشاة[1] هو جـزاء عينـي، يـنص المشرع عليـه غالبـاً كعقوبـة تكميليـة، إلى جانب ما يقضى به من عقوبات أصلية أخرى[2]. وقد ورد الـنص عـلى جـزاء الغلـق فى مجال الاعتداء على الأمن الالكتروني، بموجب المادة (41) مـن مرسـوم بقـانون اتحـادى رقم (5) لسنة 2012، حيث يحكم بإغلاق المحل، أو الموقع الـذى يرتكـب فيـه أى مـن هذه الجرائم، وذلك إما إغلاقا كليا، أو مؤقتا للمدة التى تقدرها المحكمة.

(8) الحكم بوضع المحكوم عليه تحت الإشراف أو المراقبة :

يجوز للمحكمة وفقا لنص المادة (42) من مرسوم بقـانون اتحـادى رقـم (5) لسنة 2012 فى شأن مكافحة جـرائم تقنيـة المعلومـات، أن تـأمر بوضـع المحكوم عليه تحت الإشراف أو المراقبة أو حرمانه مـن اسـتخدام أى شـبكة

(1) يتمثل غلق المنشاة فى المنع من استمرار استغلالها، وقد ثـار الجـدل حـول طبيعتهـا القانونيـة حول ما إذا كانت عقوبة خالصة، أم مجرد تدبير احترازي. راجع : د. أمـين مصـطفى محمـد : النظرية العامة لقانون العقوبات الإدارى (ظاهرة الحد من العقـاب)، دار الجامعـة الجديـدة للنشر، الإسكندرية،1996، ص 256.

(2) Merle et vitu : trait de droit criminal , quatrieme edition , 1981 , p. 870.

-A. Wlener, theory of economic criminal law Hungarian national group of international association of penal law Budapest 1984 London 1986, p. 41.

مشار إليهما لدى د. محمود عبد العزيز محمد السيد الشريف : مـدى ملائمـة الجـزاءات الجنائيـة الاقتصادية فى ظل السياسة الجنائية المعاصرة، النظرية العامـة للجـزاء الجنـائى الاقتصـادي، دراسـة تحليلية تأصيلية مقارنة، دار النهضة العربية، القاهرة، 2006-2007، ص 103.

معلوماتية، أو نظام المعلومات الالكتروني، أو أى وسيلة تقنية معلومات أخري، أو وضعه فى مأوى علاجى أو مركز تأهيل للمدة التى تراها المحكمة مناسبة.

(9) إبعاد الأجنبى :

نص المشرع الإماراتى على إبعاد الأجنبى بموجب المادة رقم (42) من مرسوم بقانون اتحادى رقم (5) لسنة 2012 فى شأن مكافحة جرائم تقنية المعلومات، بقوله " تقضى المحكمة بإبعاد الأجنبى الذى يحكم عليه بالإدانة لارتكاب أى جريمة من الجرائم المنصوص عليها فى هذا المرسوم، ويكون ذلك بعد تنفيذ العقوبة المحكوم بها".

المطلب الثاني

تقييم خطة المشرع الإماراتى فى تقرير الجزاءات

أولاً : تحديد أوجه الايجابيات المقررة :

يمكن القول أن المشرع الإماراتى ساهم كثيرا بموجب منهج اختيار الجزاءات المقررة لجرائم الاعتداء على الأمن الالكتروني، فى تحقيق كثير من جوانب العدالة، وجبر الضرر، أو الخلل الناشئ عن هذه الجرائم، كما حقق جانب كبير من فكرة الأغراض النفعية للعقوبة، من حيث تحقيق الردع العام والردع الخاص[1].

فقد لجأ المشرع إلى وسائل تفريد العقاب تشريعيا، حيث أنتهج التنويع فى العقوبات، تبعا لجسامة الجرائم إلى حد ما، فقد وضع أكثر من عقوبة أصلية عن الجريمة الواحدة، وتخويل القاضى اختيار إحداهما أو الجمع بينهما[2].

أضف إلى ذلك فقد نص المشرع على ظروف معينة، إذا ما توافرت أحد حالاتها، يشدد فيها العقوبة. كما وضع المشرع الإماراتى أيضاً العقوبات

---

(1) أنظر حول أهداف العقوبة : د. عبد الرءوف مهدى : شرح القواعد العامة لقانون العقوبات، المرجع السابق، ص 965.

(2) أنظر حول تطبيق العقوبة، وسلطة القاضى التقديرية فى تطبيقها. د. عبد الرءوف مهدى : المرجع السابق، ص 1055.

السالبة للحرية، وكذلك مقدار الغرامة المقررة فى إطار مرن، حيث قرر لها حد أقصى وحد أدني، بحيث يستطيع القاضى من خلالها توقيع الجزاء الملائم حسب ظروف الدعوي، وحسب مقدار ما تحدثه الجريمة من خلل أو استهجان[1].

ثانياً : أوجه قصور منهج تقرير الجزاءات الجنائية :

الملاحظ على منهج المشرع الإماراتى فى تقرير الجزاءات المقررة على الاعتداء على الأمن الالكتروني، أنه لم ينص على تشديد بعض العقوبات أو التدابير فى حالة (العود للجريمة).

كما لم ينص على ضرورة نشر الحكم الصادر بالإدانة، وهو جزاء يكمل الجزاء الأصلي[2]، ونادرا ما ينص عليه القانون العام، إلا أن قوانين العقوبات خصوصاً الاقتصادية كثيرا ما تنص عليه[3]. ويعد القانون الفرنسى وفقا لما لاحظه أغلب الفقهاء من أكثر التشريعات المقارنة التى تستخدم عقوبة نشر الأحكام الصادرة بالإدانة فى نطاق الجزاء المقرر خصوصاً للجرائم الاقتصادية[4].

---

(1) راجع فى هذا الصدد : د. عبد الرءوف مهدى : المرجع السابق، ص 1055 وما بعدها.

(2) يتم نشر الحكم الصادر بالإدانة سواء بالشهر على واجهة المحلات، أو بالنشر فى الصحف. أنظر فى ذلك : د.أمين مصطفى محمد : المرجع السابق، ص 266.

(3) د. محمود محمود مصطفى : الجرائم الاقتصادية، المرجع السابق، ص 176، د. مصطفى منير : جرائم إساءة استعمال السلطة الاقتصادية، الهيئة المصرية العامة للكتاب، 1992، ص 321.

(4) المادة رقم (7) من قانون قمع الغش والتدليس فى فرنسا، المعدل بموجب القانون الصادر فى 10 يناير 1978. وغيرها من أغلب الجرائم الاقتصادية فى فرنسا. راجع تفصيلاً : د. مصطفى منير : المرجع السابق، ص 321 وما بعدها.

وأخيراً، لم ينص أيضاً على جزاء فيما يتعلق بالمسئولية الجنائية عن فعل الغير، وكذلك مسئولية الأشخاص المعنوية، من خلال النص على تقرير المسئول عن الإدارة الفعلية لمنشاة أو منظمة أو مجموعة أو جمعية أو منظمة أو هيئة غير مشروعة، يثبت ارتكابها مما يعد جريمة من جرائم الاعتداء على الأمن الالكتروني.

ثالثاً: التطبيق القضائي للجزاء الجنائي المقرر ومدى فاعليته فى معالجة أوجه القصور :

يحدد المشرع العقوبة، وفقاً لمبدأ الشرعية، على أساس تناسبها مع ماديات الجريمة، ومدى خطورتها أو ضررها على المجتمع، وليس فى مقدور المشرع التكهن بالاعتبارات التى تحدد العقاب العادل والملائم، ومن ثم فإن تحقيق التناسب، والعدالة، والملائمة، لا يكون بين العقوبة والجريمة، وإنما بين العقوبة والعناصر التى يتوقف عليها تحقيق أهدافها، وهى الخطورة الإجرامية، وجسامة الجريمة[1].

ومن هنا تظهر مهمة القاضى الذى يكمل دور المشرع فى تحقيق العدالة، وفى تحقيق الجوانب الإنسانية والاجتماعية، لأن القاضى هو أكثر اتصالا بالظروف والملابسات التى أحاطت بالجريمة[2]. وهو يسترشد فى ذلك وفقا

(1) د. محمد عيد الغريب : شرح قانون العقوبات، المرجع السابق، ص 1047.

(2) د. محمد عيد الغريب : المرجع السابق، ص 1048.

لما حدده الفقه الجنائى بضابطين أساسيين هما :-

(أ) الضابط الموضوعى :

يتعلق هذا الضابط بمراعاة القاضى سلطته التقديرية إزاء المتهم، بمدى جسامة الجريمة، ومدى الاعتداء على الحق محل الحماية القانونية، حيث يراعى القاضى الاعتبارات التى تؤثر فى مقدار جسامة الاعتداء، كأسلوب تنفيذ الفعل، ووقته، ومكانه، وكافة ملابساته، وكلها اعتبارات يسترشد بها القاضى فى تحديد العدالة عن طريق النطق بالحكم الملائم(1).

(ب) الضابط الشخصى :

ترتكز الضوابط الشخصية على مراعاة القاضى درجة خطورة الإرادة المؤثمة قانوناً، حيث تتفاوت خطورة هذه الإرادة بطبيعتها فى الجريمة الواحدة من حالة لأخرى، كما تعد البواعث من أهم العوامل التى تحدد مقدار خطورتها، وبالتالى التأثير فى مجال السلطة التقديرية للقاضى عند اختياره للعقوبة الملائمة لجسامة الجريمة(2).

---

(1) د. محمد عيد الغريب : المرجع السابق، ص 1052. ؛ د. أحمد عوض بلال : محاضرات فى الجزاء الجنائي، دار النهضة العربية، القاهرة، 2000-2001، ص 330. ، د. حاتم بكار : حماية حق المتهم فى محاكمة عادلة، دراسة تحليلية تأصيلية انتقاديه مقارنة، منشأة المعارف، الإسكندرية، 1997، ص 505 وما بعدها.

(2) د. محمد عيد الغريب : المرجع السابق، ص 1053. ؛ د. أحمد عوض بلال : المرجع السابق، ص 331.

موقف المحكمة الاتحادية العليا الإماراتية من الضوابط الشخصية والموضوعية :

تطبيقاً للضوابط الموضوعية والشخصية السالفة البيان، فقد قضت المحكمة الاتحادية العليا فى دولة الإمارات العربية المتحدة، وقد جاء فى حكمها أنه مراعاة ظروف المتهم الشخصية، ومن ثم فإن المحكمة تعامله بشئ من الرحمة وتخفف عنه العقوبة إعمالاً للمادة (98) من قانون العقوبات الاتحادي. وكان ذلك بصدد جريمة استخدام بطريق العلانية وسيلة من وسائل تقنية المعلومات فى بث دعايات مثيرة لعامة الناس بأن نشر المتهم مقطعاً مصوراً احتوى على عبارات وتهديدات. عن طريق استحداث موقع جديد على (اليوتيوب) بشبكة الانترنت، وبث فيه مقطع فيديو أنتجه للترويج لأفكار من شأنها الإخلال بالآداب العامة وبالنظام العام بإلقاء الرعب والهلع بين الناس[1].

(1) أنظر : حكم المحكمة الاتحادية العليا فى دولة الإمارات العربية المتحدة، فى القضية رقم (2) لسنة 2012 جزائى أمن دولة، جلسة الاثنين الموافق 26 من مارس سنة 2012. وقد ورد فى مضمون هذا الحكم ضمن الوقائع التى عرضت لها المحكمة فى الحكم، أن الشاهد وهو والد المتهم ذكر أن ابنه تعرض للاعتداء بطعنات بسلاح أبيض بمدينة دبى قبل حوالى 6 أشهر، وأن القصد من مقطع الفيديو كما ورد فى أقوال المتهم هو إنتاج أغنية راب دون قصد نشر الرعب فى المجتمع، وحيث انه بتفريغ القرص المدمج المضبوط الحامل الرقم التسلسلى .... من طرف الخبير المهندس/ ... من الإدارة العامة للأدلة الجنائية وعلم الجريمة، وتضمن بالخصوص صورة يشاهد فيها أشخاص بصدد الاعتداء بالعنف على شخص وكتب على الصورة " ها بيكون مصير كل واحد يسب أو يتزعم على "دنجور"، وصورة أخرى تظهر وجه شاب تكسوه الدماء وكتب على الصورة "والله لأعذبه مثل ما عذبت غيره".

الفصل الثالث

الحماية الجنائية الإجرائية للأمن الالكتروني

تمر إجراءات الحماية الجنائية للأمن الالكتروني، بثلاث مراحل أساسية. الأولى هي مرحلة التحرى والاستدلال، والثانية التحقيق الابتدائي، والثالثة المحاكمة، وسوف نركز على أوجه الخروج عن القواعد العامة فى هذه الإجراءات، فى نطاق حماية الأمن الالكتروني.

المبحث الأول : ذاتية قواعد التحرى والاستدلال بشأن الاعتداء على الأمن الالكتروني.

ذاتية إجراءات التحقيق الابتدائى بشأن الاعتداء على الأمن الالكتروني.

ذاتية إجراءات المحاكمة بشأن الاعتداء على الأمن الالكتروني.

المبحث الثاني: المبحث الثالث :

المبحث الأول

ذاتية قواعد التحرى والاستدلال

بشأن الاعتداء على الأمن الالكتروني

تقوم الضبطية القضائية بالبحث عن الجرائم ومرتكبيها وجمع الاستدلالات التى تلزم للتحقيق والدعوي[1]. فعملها لا يبدأ إلا بعد وقوع الجريمة، وبقصد الوصول إلى معاقبة فاعلها، وهى بالطبع تختلف عن الضبطية الإدارية، وهذه الأخيرة مهمتها منع وقوع الجرائم[2]. وسوف نعالج ذلك فى مجال الاعتداء على الأمن الالكترونى فى النقاط التالية :

أولاً: تحديد ضبطية قضائية خاصة للتحرى والاستدلال :

تتجه السياسة الجنائية الحديثة فى التشريعات المقارنة، ومنها المشرع الإماراتي، إلى تخصيص ضبطية قضائية خاصة تعنى بالبحث والتحرى والاستدلال عن الجرائم الالكترونية، وتجد هذه السياسة مبرراتها فى أن هذه الجرائم بطبيعتها معقدة، وتحتاج إلى دراية فنية خاصة فى الكشف عنها[3]،

(1) المادة رقم (21) من قانون الإجراءات الجنائية المصري.

(2) أنظر : د. محمود محمود مصطفى : شرح قانون الإجراءات الجنائية، الطبعة الثانية عشرة، القاهرة، 1988، ص 207، بند (156).

(3) راجع فى هذا الصدد : د. محمود محمود مصطفى : الجرائم الاقتصادية فى القانون المقارن، مرجع سابق، ص 226.

وفيما يلى بيان منهج المشرع الإماراتى :

(1) أداة منح صفة الضبطية القضائية الخاصة :

الضبطية القضائية الخاصة هم من يقومون بوظيفة الضبطية فى جرائم معينة تتعلق عادة بالوظائف التى يؤدونها، فليس لهم مباشرتها خارج هذا النطاق[1]. وقد منح المشرع الإماراتى صفة الضبطية القضائية الخاصة لبعض الموظفين لدى الجهات الاتحادية، أو المحلية، المعنية بشؤون الأمن الالكترونى فى الدولة، وقد قرر المشرع أن منح هذه الصفة يكون بقرار من وزير العدل، بالاتفاق مع رئيس مجلس إدارة الهيئة الوطنية للأمن الالكتروني[2].

(2) الجزاء الإجرائى المترتب على مباشرة الضبط العام للمهام المسندة إلى الخاص:

جرى العمل على أن أصحاب صفة الضبطية القضائية العام، لا يباشرون وظيفة الضبطية القضائية الخاصة، ولكن رغم ذلك فإن مباشرتهم لها وفقا لرأى البعض من الفقه ووفقا لما يؤيده الباحث يكون صحيحا[3].

---

(1) أنظر : د. محمود محمود مصطفى : المرجع السابق، ص 209، بند (160).

(2) راجع المادة رقم (1) من مرسوم بقانون اتحادى رقم (3) لسنة 2012م، بإنشاء الهيئة الوطنية للأمن الإلكتروني. والمادة الأولى من مرسوم بقانون اتحادى رقم (5) لسنة 2012م، فى شأن مكافحة جرائم تقنية المعلومات، فى دولة الإمارات العربية المتحدة.

(3) أنظر فى ذلك : د. محمود محمود مصطفى : المرجع السابق، ص 210، بند (160).

ذلك لأنه لا يوجد نص يحظر ذلـك، كـما لا يوجـد نـص بموجـب قـانون إنشـاء الهيئـة الوطنيـة للأمـن الالكـتروني، أو بموجـب قـانون مكافحـة جـرائم تقنيـة المعلومـات، فى التشريع الإماراتى يقرر بموجبه المشرع اختصاص استئثارى لأعضـاء الضـبطية القضـائية الخاصة، لذلك لا يترتب على مخالفة قواعد هذا الاختصاص بطلان الإجراءات.

(3) نطاق وحدود اختصاص عضو الضبط القضائى :

أكد المشرع الإماراتى بموجب المادة رقم (14) من مرسوم بقانون اتحادى رقـم (3)، على أنه يتحدد نطاق اختصاص الهيئة، فيما يلزم لتفادى الاعتداء على الأمن الالكتروني، سواء كان ذلك من داخل دولة الإمارات، أو من خارجها. وهذا الاتجاه محمود من قبل المشرع الإماراتي، لكون أن أغلب جرائم الاعتداء عـلى الأمـن الالكـترونى تـرتبط بأمـاكن وأجهزة وأنظمة عديدة قد تتعدى حدود الدولة الواحدة.

(4) واجبات ومهام وسلطات أعضاء الضبطية القضائية الخاص :

يرى البعض من الفقه أن رجل الضبط القضائى لـه أن يـدخل الأمـاكن العامة على شبكة الانترنـت التـى للشـخص العـادى أن يـدخلها كـالمواقع المختلفة، وتصح الإجراءات ويجوز الاستناد إليهـا كـدليل، بيـد أنـه لـيس لرجل الضبط أن يستعين بـبرامج اخـتراق الـدخول إلى المواضـع الخاصـة،

(كالايميل والماسنجر)[1]...الخ.

ويأتى هذا الرأى متوافقاً فيما قضى به القضاء الفرنسى بأن لرجل الضبط أن يتصل بشبكة الميناتل، وأن يقرأ ما عليها من رسائل دون تعديل فى تجهيزها شأنه فى ذلك شان الشخص العادي[2]. وفى هذا الصدد فقد أوجب المشرع الإماراتى على السلطات المحلية بدولة الإمارات العربية المتحدة، تقديم التسهيلات اللازمة لأعضاء الضبطية القضائية الخاصة[3]. وهذا الاتجاه ضرورى ولازم للبحث والتحرى والكشف عن الجرائم الالكترونية، نظرا لخطورتها.

ثانياً : آليات وسبل تحقيق الأمن الالكترونى فى القانون الإماراتى :

يستفاد مما نصت عليه المادتين أرقام (13-14) من المرسوم بقانون اتحادى رقم (3) لسنة 2012، أن سبل تحقيق الحماية للأمن الإلكترونى فى الحالات العادية، يكون عن طريق تدخل السلطات أو الجهات المختصة[4]

---

(1) أنظر هذا الرأى : د. غنام محمد غنام : المرجع السابق، ص 173.

(2) Crim.25 oct. 2000, Bull. Crim. No 317; Penal 2001. Comm. 27, obs. Maron.

(3) المادة (49) من مرسوم بقانون اتحادى رقم (5) لسنة 2012م، فى شأن مكافحة جرائم تقنية المعلومات.

(4) الجهات المختصة أو الجهات المعنية بهذا الشأن وفقاً للقانون الإماراتى هى الجهات الاتحادية، أو المحلية المعنية بشؤون الأمن الالكترونى داخل الدولة، أو غير ذلك من الجهات التى يصدر بتحديدها قرار بعد ذلك. راجع المادة الأولى من مرسوم بقانون اتحادى رقم (3) لسنة 2012، والمادة الأولى من مرسوم اتحادى رقم (5) لسنة 2012.

باتخاذ أيا من الإجراءات التالية :

(1) مراقبة شبكة الاتصالات ونظم المعلومات :

أجازت المادة رقم (13) من مرسوم بقانون اتحادى رقم (3) لسنة 2012م، للجهة المختصة اتخاذ كل ما يلزم لمراقبة عدم تعرض شبكة الاتصالات، ونظم المعلومات فى الدولة، لأى عمليات دخول غير مشروعة، أو كشف مواقع الخلل فى شبكة الاتصالات ونظم المعلومات.

(2) منع وإعاقة وتعطيل شبكة الاتصالات ومحتوى نظم المعلومات :

ويتم ذلك عن طريق قيام السلطة أو الجهة المختصة بوضع الضوابط اللازمة لمنع أى محاولات تهدف إلى تعطيل، أو تخريب، أو تغيير، أو منع الوصول غير المصرح به للشبكة المعلوماتية، أو شبكة الاتصالات، أو محتوى نظم المعلومات[1].

والجدير بالإشارة إليه أن وسيلة تحقيق الأمن الالكترونى التى تتم بمعرفة السلطة المختصة، يكون عن طريق استخدام إحدى الوسائل الالكترونية المتعارف عليها، وهى تشمل بصفة خاصة كل ما يتصل بالتكنولوجيا (الكهرومغناطيسية، أو الكهروضوئية، أو الرقمية، أو مؤتمتة، أو ضوئية)، أو ما شابه ذلك[2]. أو بمعنى اشمل كل ما يتصل بالتكنولوجيا

(1) راجع المادة رقم (1) والمادة رقم (14) من مرسوم بقانون اتحادى رقم (3) لسنة 2012م، بإنشاء الهيئة الوطنية للأمن الإلكتروني.

(2) راجع : المادة الأولى من مرسوم بقانون اتحادى رقم (5) لسنة 2012م.

الحديثة ويكون ذات قدرات كهربائية أو رقمية أو مغناطيسية أو لاسـلكية أو بصريـة، أو كهرومغناطيسية أو مؤتمته[1] أو ضوئية أو ما شابه ذلك[2].

---

(1) الوسيط أو المعاملات الالكترونية المؤتمته هو عبارة عن برنامج أو معاملـه أو نظـام إليكـتروني لوسيلة تقنية المعلومات تعمل تلقائيا بشكل مستقل، كليا أو جزئيا، دون إشراف أو متابعة أو مراجعة من أى شخص طبيعي. أنظر فى ذلك : المادة رقم (1) من القانون الاتحـادى رقـم (1) لسنة 2006 فى شأن المعاملات والتجارة الإلكترونية، فى دولة الإمارات العربية المتحدة.

(2) المـادة رقـم (1) مـن القـانون الاتحـادى رقـم (1) لسـنة 2006 فى شـأن المعـاملات والتجـارة الإلكترونية، فى دولة الإمارات العربية المتحدة.

المبحث الثاني

ذاتية إجراءات التحقيق الابتدائى

بشأن الاعتداء على الأمن الالكتروني

يهدف التحقيق إلى التثبت من الأدلة القائمة على نسبة الجريمة إلى فاعل معين، لذلك فإن الدليل القانونى هو ما يستمد من التحقيق، وقد اشترط القانون أن يؤدى هذا الإجراء وفقاً لأوضاع وإجراءات وضمانات معينة، وتشمل أهم إجراءات التحقيق التفتيش وضبط الأشياء المتعلقة بالجريمة، وسماع الشهود، وندب الخبراء[1]، ...الخ. وسوف نركز على بعض من هذه الإجراءات فقط فى مجال جرائم الاعتداء على الأمن الالكتروني، والتى يثار بشأنها المشكلات، وسيكون معالجة ذلك فى النقاط المحددة التالية :

أولاً : حرمة الحياة الخاصة والأمن الالكترونى :

لا شك أن الرسائل، والمستندات، وأنظمة المعلومات الالكترونية ومحتوياتها الخاصة، تتعلق بحرمة الحياة الخاصة للأفراد، لذلك فإن مراقبتها وتسجيلها، تخضع بالضرورة للضمانات المقررة بموجب قانون الإجراءات الجزائية الإماراتي، ومنها ضرورة صدور إذن من النيابة، وغيرها من

---

(1) أنظر : د. محمود محمود مصطفى : شرح قانون الإجراءات الجنائية،المرجع السابق، ص 207 ، ص 259، ص 272.

الضمانات الأخرى[1].

ويرى البعض من الفقه أنه رغم اختلاف المراسلات البريدية عن الالكترونية، ونظرا لتعلق هذا الأمر بحرمة الحياة الخاصة، فإنه يتعين أن يتدخل المشرع بنص صريح على سريان ذات الضمانات المقررة بموجب قانون الإجراءات الجزائية فيما يتعلق بالمراسلات البريدية، على المرسلات الالكترونية[2].

ونشير فى هذا الصدد، أن هناك بعض التشريعات الحديثة بالفعل كالتشريع الأمريكي، سوى بين اعتراض الاتصالات السلكية، والالكترونية[3]. من حيث كونها تتعلق بحرمة الحياة الخاصة وأن الاعتداء عليها يمثل جريمة.

ثانياً : التفتيش والضبط بشأن جرائم الأمن الالكترونى :

إن غاية التفتيش هى الضبط[4]. والتفتيش هو البحث عن الحقيقة فى مستودع السر، وقد يشمل هذا الإجراء الأشخاص المتهمين، أو المساكن، أو الأمتعة[5]، ..الخ. ولا يجوز لمأمور الضبط القضائى أن يقوم بالتفتيش بدون

(1) المواد (65-131 إجراءات جزائية اتحادي).

(2) د. غنام محمد غنام : المرجع السابق، ص 191.

(3) 2511, Sec. 119, Part I, Chapter 18 title. (Intentionally intercepts any wire. oral or electronic connunication.

(4) أنظر : د. محمود محمود مصطفى : شرح قانون الإجراءات الجنائية، المرجع السابق، ص 283.

(5) أنظر فى ذلك : د. احمد شوقى عمر أبو خطوة : المبادئ العامة فى قانون الإجراءات الجنائية، القاهرة، 2011، ص 349 وما يليها.

إذن قضائي، إلا فى حالات التلبس[1]. كما لا يصح قانونا هذا الإجراء - وهو من إجراءات التحقيق- إلا لضبط جريمة واقعة بالفعل وترجحت نسبتها إلى متهم معين، كما لا يصح اتخاذ هذا الإجراء لضبط جريمة مستقبلة، ولو قامت التحريات والدلائل الجدية على أنها ستقع بالفعل[2]. وسوف نبين هذه الأحكام بالتطبيق على جرائم الاعتداء على الأمن الالكترونى فى النقاط التالية :

(1) البطلان الذاتى للدليل لعدم مراعاة الضمانات الإجرائية فى التحقيق :

أحاط المشرع الإماراتى إجراءات ضبط الرسائل، ومراقبة المحادثات السلكية واللاسلكية، وتسجيلها بضمانات جوهرية، من أهمها الحصول على موافقة النائب العام[3].

ومن ثم يترتب البطلان على عدم مراعاة أحكام التفتيش والضبط، فى هذا النطاق وهو نوع من البطلان الذاتى للإجراء[4] Nullite substantielles.

---

(1) المادة (53) من قانون الإجراءات الجزائية الإماراتي.

(2) د. محمود محمود مصطفى : شرح قانون الإجراءات الجنائية، المرجع السابق، ص 275. وأنظر (نقض أول يناير سنة 1962 مجموعة أحكام النقض، س 13، رقم 5، ص 20)

(3) (م 75 إجراءات جزائية).

(4) البطلان الذاتى : مؤداه أن يترك للقاضى تقدير الأحوال التى يترتب البطلان فيها، وليس المشرع هو الذى يقدر مدى أهمية الشكل الذى خولف. أنظر :

Merle- Vitu, Procedure Penal, 1984, P. 543.

وهناك ما يسمى بالبطلان القانوني، ومؤداه أن تقرير مثل هذا البطلان، لا يكون إلا بنص خاص من المشرع، فلديهم أنه لا بطلان بغير نص. أنظر :

Stefani, Levasseur, Bouloc, Procedure Penal, 1984, P. 689.

ورغم ذلك فإن بطلان التفتيش لا يؤثر على الإجراءات السابقة أو اللاحقة عليه، فتصح إدانة المتهم بناء على أدلة أخري، ومنها اعترافه إذا تـوافرت شروط صحته، ولم يكـن نتيجة حتمية للتفتيش الباطل[1].

وتطبيقاً لذلك فقد قضت المحكمة الاتحادية العليا فى دولة الإمارات، بإدانة مـتهم بناء على اعترافه بتعمد استعمال وسيلة من وسائل تقنية المعلومات (اليوتيوب عـلى شبكة الانترنت) لإنتاج مقطع فيديو مخيف، حتى يجعل لنفسه هالة تخيف النـاس وتبعث فى قلوبهم الرعب والهلع والخوف[2].

(2) الرضا بالتفتيش فى جرائم الأمن الالكترونى :

بالإضافة إلى حالة الإذن، وحالة التلبس، مـن المقـرر أنـه يجـوز تفتـيش الأشـخاص والأماكن – ما لم يكن مسكنا فى القانون المصري- استنادا إلى رضاء صاحب الحق، وهذه القاعدة وجدت تطبيقا لها فى مجال الاعتداء على الأمن الالكتروني، من جانـب القضـاء الأمريكي، بل ذهب إلى أبعد من هذا. فقـد قـرر هـذا القضـاء فى أحـد أحكامـه أنـه لا يستلزم أن يصدر الرضاء من صاحب النظـام نفسـه، بـل يكفـى أن يكـون مـن شـخص يستعمل هذا النظام، فالعبرة بالاعتياد على استعمال الجهاز وليس بملكية الجهاز[3].

---

(1) أنظر : د. محمود محمود مصطفى : شرح قانون الإجراءات الجنائية، المرجع السابق، ص 293. وأنظر كذلك (نقض 22 نوفمبر سنة 1945 مجموعة أحكام النقض المصرية، س 6، رقم 67، ص 201)

(2) حكم المحكمة الاتحادية العليا، القضية رقم (2) لسنة 2012 جزائى أمـن دولـة، جلسـة الاثنـين الموافق 26 من مارس سنة 2012.

(3) United States V. Smith, 27 F. Supp. 2d 111, 16-1115 (C.D. III. 1998). www.cybercrime.gov/smanual 2002.htm

وأخيراً نشير إلى أن القضاء الأمريكى يسوى بين البريد العادي، والبريد الإلكترونى من حيث الضمانات المتعلقة بالتحقيق. فقد قضى ببطلان الدليل المستمد من دخول رجال الضبط القضائى إلى البريد الإلكترونى للمتهم وحصولهم على دليل لإثبات ارتكاب الجريمة لعدم حصولهم على إذن قضائي، ولعدم توافر رضاء صاحب البريد نفسه[1].

ثالثاً : الأحكام الإجرائية الخاصة بالأمن الالكترونى فى التشريع الإماراتى :

تضمن قانون الإجراء الجزائية الإماراتى أحكام خاصة بشأن الاتصالات الهاتفية. فقد نصت المادة (75) إجراءات جزائية اتحادى على أنه " لعضو النيابة العامة... أن يراقب المحادثات السلكية واللاسلكية متى استوجبت مقتضيات التحقيق ذلك". إلا أنه فى مجال تحقيق الأمن الالكترونى فى الحالات الاستثنائية (الطارئة أو المستعجلة) انتهج المشرع سياسة إجرائية يهدف بها تحقيق المصالح الهامة ذات الصلة بالأمن الالكتروني، وسوف نبين ذلك من خلال النقاط التالية :

---

(1) U.S. c.Maxwell 45 MJ 406 , 1996; Rene PEPIN, Le statut juridique du cornel au Canada et aux Etats- Unis, www. Lex-electronica. Org/articles/v 2-6/pepin.htm

راجع : د. غنام محمد غنام : المرجع السابق، ص 191.

(أ) آليات تحقيق الأمن الالكترونى فى الحالات الطارئة أو المستعجلة :

(1) تحديد إجراءات وضرورات التدخل الطارئ أو العاجل :

منح المشرع الإماراتى للسلطة المعنية أو المختصة- وهى الهيئة الوطنية للأمن الالكتروني- فى الحالات الطارئة أو المستعجلة بشأن منع الاعتداء على الأمن الالكتروني، صلاحية (مراقبة، أو اختراق، أو معالجة، أو إلغاء، أو تعطيل، أو حجب شبكة الاتصالات ونظم المعلومات وأجهزة الاتصالات والرسائل الالكترونية) بأى شخص، أو جهة. إلا أن المشرع الإماراتى حدد ضوابط هذا التدخل، إذا تبين للجهة المختصة أن هذا الشخص، أو الجهة اشترك فى أى عمل من شأنه أن يؤثر على الآتي[1]:ــ

- أمن الدولة، أو عقيدتها، أو اقتصادها، أو تراثها أو حضارتها.
- النظام العام، أو السلم الاجتماعي.
- العلاقات الدولية والإقليمية.
- المنشآت الحيوية والجهات العامة أو الخاصة العاملة فيها.
- حياة أو أموال أى شخص متواجد بالدولة.

ويبدو مما سلف أنه بقدر خطورة إجراءات التدخل من حيث شمولها

(1) راجع المادة (14-2) من مرسوم بقانون اتحادى رقم (3) لسنة 2012م، بإنشاء الهيئة الوطنية للأمن الإلكتروني، فى دولة الإمارات العربية المتحدة.

لأفعال تتمثل فى الاختراق، والمعالجة، والإلغاء، والتعطيل والحجب للنظام، إلا أنه على قدر هذه الخطورة يقابلها أهمية المصلحة المعتدى عليها أيضا، حيث تتضمن مصالح عليا كأمن الدولة، والنظام العام، والعلاقات الدولية...الخ.

(ب) الضوابط والضمانات الإجرائية لحالات التدخل الطارئ أو العاجل :

لم يترك المشرع الإماراتى صلاحية الهيئة فى اختراق، أو إلغاء، أو تعطيل، أو حجب شبكة الاتصالات ونظم المعلومات والرسائل الالكترونية، ...وغيرها على النحو السالف البيان، دون قيود أو ضمانات، وإنما حدد هذه الأخيرة فى الآتى :

(1) استطلاع رأى مستشار الأمن الوطنى :

أشار المرسوم بقانون اتحادى رقم (3) لسنة 2012، فيما تضمنته المادة رقم (14-2) من هذا المرسوم إلى أنه يلزم للإجراءات التى تتخذ فى الحالات الطارئة أو المستعجلة، لمنع الاعتداء على الأمن الالكتروني، استطلاع رأى مستشار الأمن الوطني.

(2) إخطار النيابة العامة المختصة :

تطلبت المادة رقم (2/14) من المرسوم بقانون اتحادى رقم (3) لسنة 2012 أنه فى الحالات المستعجلة التى تبرر ضرورات الدخل الطارئ

بالإجراءات السالفة البيان، أن يتم إخطار النيابة العامة المختصة بالإجراء الذى اتخذته الهيئة فى هذه الحالات، خلال أسبوع لإعمال شئونها حيال هذا الإجراء[1].

ويبدو أن حالات وضرورات التدخل الطارئ، من قبل الهيئة الوطنية للأمن الالكتروني، على النحو السالف البيان، هى مسالة تقديرية للهيئة، ولكنها تخضع لرقابة القضاء فيما بعد. أضف إلى ذلك أن النيابة العامة - وفقا لمؤدى المادة (14) من القانون (3) لسنة 2012- لها حرية إعمال شئونها حيال الإجراءات التى اتخذتها الهيئة. وهو ما يقرر نوع من الرقابة التى تمارسها النيابة العامة على صحة الإجراءات التى اتخذتها الهيئة.

(1) المادة (14-2) من مرسوم بقانون اتحادى رقم (3) لسنة 2012م، بإنشاء الهيئة الوطنية للأمن الإلكتروني، فى دولة الإمارات العربية المتحدة.

المبحث الثالث

ذاتية إجراءات المحاكمة بشأن الاعتداء على الأمن الالكتروني

أولاً : البعد الدولى لجرائم الاعتداء على الأمن الالكترونى :

تعتبر جرائم الاعتداء على الأمن الالكترونى من الجرائم ذات البعد الدولي[1]. ذلك لأن اغلب هذه الجرائم، كالدخول إلى موقع الكترونى لإعاقته أو تعطيله، أو الإدخال العمدى لنظام الكتروني، بقصد الحصول على بيانات حكومية، أو معلومات سرية خاصة بمنشأة مالية أو تجارية أو اقتصادية .... الخ. قد ترتكب أو تترتب آثارها، أو نتائجها الخطرة أو الضارة فى مكان آخر، أو فى دولة أخرى غير التى ارتكب فيه السلوك، فضلاً عن أنه قد تكون جنسية مرتكبها، أو المجنى عليه فيها أجنبياً.

وهذه المسألة تثير كثير من المشكلات فيما يتعلق بتحديد المحكمة المختصة بنظر الدعاوى الجنائية الناشئة عن هذه الجرائم، إذا ما اتخذت بالطبع بعداً دوليا بسبب جنسية الجاني، أو جنسية المجنى عليه، أو بسبب

(1) أنظر فى هذا الصدد : د. غنام محمد غنام : المرجع السابق، ص 204. وهذه الجرائم رغم أنها تتخذ بعد دولى إلا أنها ليست جريمة دولية، لأن هذه الأخيرة لها تعريف لا يرى على هذا النوع من الجرائم، لكون الجريمة الدولية تمس مصلحة جوهرية للمجتمع الدولى كالجرائم ضد السلام، والجرائم ضد الإنسانية، وجرائم الحرب. أنظر : د. محمود نجيب حسنى : دروس فى القانون الجنائى الدولي، دار النهضة العربية، القاهرة، 1959-1960، ص 45 وما بعدها.

الإقليم الذى ارتكبت فيه[1].

ثانياً : ضوابط الاختصاص بجرائم الأمن الالكترونى فى التشريع الإماراتي:

يفهم الاختصاص بأنه مباشرة المحكمة ولايتها القضائية فى نظر الدعوى فى الحدود التى رسمها القانون[2]. ولا تكون المحكمة الجنائية مختصة بنظر الدعوى المرفوعة إليها إلا إذا كانت مختصة بالنسبة لشخص المتهم، ومن حيث نوع الجريمة المسندة إليه، ومن حيث المكان[3]. ومن المعلوم أيضاً أنه يسود النطاق المكانى لقانون العقوبات مبدأ إقليمية القانون الجنائي، الذى يعنى أن قانون العقوبات يطبق على إقليم الدولة التى أصدرته[4].

إلا أن المشرع الإماراتي، خرج على هذه القاعدة فيما يتعلق بجرائم الاعتداء على الأمن الالكتروني، وانتهج مبدأ العينية[5]. حيث نص المشرع بموجب المادة رقم (47) من قانون مكافحة جرائم تقنية المعلومات على أنه

---

(1) أنظر : د. محمد عيد الغريب : المرجع السابق، ص 1107.

(2) د. احمد شوقى عمر أبو خطوة : المبادئ العامة فى قانون الإجراءات الجنائية، المرجع السابق، ص 482.

(3) د. محمود محمود مصطفى : شرح قانون الإجراءات الجنائية، المرجع السابق، ص 351.

(4) د. عبد الرءوف مهدى : محاضرات فى قانون العقوبات الاقتصادي، دار النهضة العربية، القاهرة، 2007-2008، ص 15. وراجع المادة رقم (16) من قانون العقوبات الاتحادي.

(5) مقتضى هذا المبدأ تطبيق القاعدة الجنائية الوطنية على الجرائم التى تمس مصلحة أساسية للدولة، أو تهدد كيانها أيا كانت جنسية مرتكبها أو مكان وقوعها. أنظر : د. عبد العظيم مرسى وزير : شرح قانون العقوبات، القسم العام، المرجع السابق، ص 100.

" ... تسرى أحكام هذا المرسوم بقانون على كل من ارتكب إحدى الجـرائم الـواردة بـه خارج الدولة، إذا كان محلها نظام معلوماتى الكـتروني، أو شـبكة معلوماتيـة، أو موقـع الكتروني، أو وسيلة تقنية معلومات خاصة بالحكومة الاتحاديـة، أو احـدى الحكومـات المحلية لإمارات الدولة، أو إحدى الهيئات أو المؤسسات العامة المملوكة لأى منها".

ومن هنا فقد اعتبر المشرع الإماراتي، أن الاعتداء على الأمن الالكترونى فـيما يتصـل بالحكومة، أو احدى الهيئات والمؤسسات العامة، مصـلحة أساسـية وجوهريـة للدولـة، تهدد كيانها، لذلك قرر الخروج عـن القواعـد العامـة فى شـأن مبـدأ الإقليميـة. ويؤيـد علـماء القـانون الجنـائى وبحـق هـذا الاتجـاه بوجـه عـام خصوصـا فى مجـال الجـرائم الاقتصادية[1].

ثالثاً : صعوبة الإثبات الجنائى فى مجال الاعتداء على الأمن الالكترونى :

(1) ذاتية الدليل الالكترونى فى مجال إثبات الاعتداء على الأمن الالكترونى :

تتميز الأدلـة الالكترونيـة، أو مـا يطلـق عليهـا الـبعض أحيانـاً الأدلـة الرقمية، بعدة خصائص من حيث أنها فى أغلب الأحيـان مـن الأدلـة غـير الملموسة، لـذلك فـإن إدراكهـا يحتـاج إلى الاسـتعانة بـأجهزة، ومعـدات، وأدوات، ونظم وبرمجة حاسوبية، كما تتميز هذه الأدلة خصوصاً فى ظـل

---

(1) أنظر فى بيان ذلك تفصيلاً د. عبد الرءوف مهدى : المرجع السابق، ص 17. د. السعيد مصطفى السعيد : مجموعة المحاضرات التى ألقيت على طلبة الدراسات العليا فى الجـرائم الاقتصـادية، 1967، ص 49.

التقدم التقنى بإمكان استرجاعها بعد محوها، وإصلاحها بعد إتلافها، وإظهارها بعد إخفائها، مما يصعب الخلاص منها، حيث توجد العديد من البرامج الحاسوبية وظيفتها استعادة البيانات بعد الحذف، كما أن الأدلة الرقمية ذات طبيعة ديناميكية فائقة السرعة، تنتقل من مكان لآخر عبر شبكات الاتصال متعدية لحدود الزمان والمكان[1].

وعلى ضوء ما سلف ذكره من خصائص، فإن مظاهر صعوبة إثبات هذه الأدلة، والتعويل عليها فى الأحكام القضائية، تكمن فى مدى الحاجة إلى أهل الخبرة من الفنيين والمتخصصين، ومدى صلاحية الدليل ذاته نظراً لطبيعته الخاصة فى تكوين عقيدة القاضى وقناعته الشخصية.

(2) حتمية الاستعانة بالخبرة الفنية فى مجال إثبات الاعتداء على الأمن الالكتروني:

لم تفرض التشريعات المقارنة على القاضى الجنائى ضرورة الاستعانة بأهل الخبرة فى مجال الاعتداء على الأمن الالكتروني. فالقاضى هو الخبير الأعلى[2]. ومع ذلك فإن الطبيعة المعقدة لجرائم الاعتداء على الأمن الالكتروني، على نحو ما ذكرنا آنفا، تفرض وتحتم على القاضى الاستعانة بأهل الخبرة من المتخصصين.

---

(1) أنظر : خبير/ عبد الناصر محمد محمود فرغلى ، د. محمد عبيد سيف سعيد المسمارى : المرجع السابق، ص 14 وما يليها.

(2) د. محمود محمود مصطفى : الجرائم الاقتصادية فى القانون المقارن، المرجع السابق، ص 86.

وقد وجدت هذه الفكرة تكريسا قضائياً لها فى أغلب الأحكام القضائية المتعلقة بجرائم الاعتداء على الأمن الالكتروني. فقد قررت محكمة النقض الفرنسية فى أحد أحكامها انه من الضرورى الاستعانة بأهل الخبرة فيما يتعلق بجرائم تقنية المعلومات[1]. وكذلك ما تبين أيضاً من اتجاه حكم المحكمة الاتحادية العليا الإماراتية فى أحد أحكامها[2]. وما سارت عليه اتجاهات أحكام المحكمة الاقتصادية الجنائية فى مصر[3].

ثالثاً : التعاون الدولى فى مواجهة جرائم الاعتداء على الأمن الالكترونى :

(1) أهمية وضرورة التعاون الدولى :

يرى بعض الفقه الجنائى أنه من الضرورى أن يتم تنظيم التعاون الدولى فى مجال مكافحة جرائم تقنية المعلومات، بوجه عام، وتشمل مظاهر هذا

---

(1) حيث أدانت متهم فى جريمة استيراد برامج مزيفة ومزورة بالمخالفة لأحكام المادة 3/355 والمادة 3/6/122 الفقرتين 1 و 2 من قانون الملكية الفكرية الفرنسي، وبنت المحكمة حكمها على ما انتهى إليه تقرير هذا الخبير، من أن التقليد كان بطريقة توحى للمستهلك بما لا يدع مجالا للشك، بأن هذا المنتج المزيف هو ذاته المنتج الأصلي. انظر :

Cour de Cassation chambre criminelle Arrêt du 6 février 2001.

(2) حيث ورد فى حكمها أنه تم تفريغ القرص المدمج المضبوط الحامل الرقم لسلىسالت GBS 601E 93 D281A80من طرف الخبير المهندس من الإدارة العامة للأدلة الجنائية وعلم الجريمة.

انظر القضية رقم (2) لسنة 2012 جزائى أمن دولة، جلسة الاثنين الموافق 26 من مارس سنة 2012.

(3) حيث أدانت المتهم بناء على الأدلة المتحصل عليها بالفحص الفنى بمعرفة قسم المساعدات الفنية بفحص البريد الالكترونى لكل من المجنى عليها والمتهم. الدعوى رقم (26) لسنة 2008، جنح كلى اقتصادي، جلسة السبت 31 يناير 2009.

التعاون المساعدة بين أجهزة الضبط، والتحقيق، والمحاكمة، بل من الممكن أن يرقى التعاون إلى إيجاد نوع من التقارب التشريعى فى مجال تجريم أفعال الاعتداء على الأمن الالكتروني[1]. وهذه الرؤية بلا شك تفرضها الطبيعة والذاتية الخاصة لجرائم تقنية المعلومات والاتصالات، التى على ما يبدو أصبحت تستقل عن الجرائم العادية، بذاتية موضوعية، وكذلك إجرائية.

(2) عوائق ومشكلات التعاون الدولى :

حدد الفقه الجنائى بعض من عوائق التعاون الدولى فى مجال مواجهة جرائم الاعتداء على الأمن الالكتروني، أو جرائم تقنية المعلومات بوجه عام، وتتمثل أهم مظاهر هذه العوائق من صعوبة معرفة الفاعل فى هذه الجرائم أحيانا، بالإضافة إلى وقوع هذه الجرائم غالباً خارج الدولة التى يحدث فيها الاعتداء، حال كون أن هذه الجرائم لا يوجد اتفاق أو توافق بين الدول على تجريم ذات الأفعال، وأخيرا عدم وجود اتفاقيات دولية لتسليم المجرمين فى هذا النوع من الإجرام[2].

رابعاً : مدى الحاجة إلى قضاء متخصص فى مجال جرائم تقنية المعلومات :

تتجه السياسة التشريعية الحديثة إلى مبدأ التخصص القضائي. من ذلك مثلاً المشرع البلاروسى الذى أنشأ المحاكم الاقتصادية، وأسند إليها

---

(1) أنظر فى هذا الرأى : د. غنام محمد غنام : المرجع السابق، ص 218 وما يليها.

(2) راجع : د. غنام محمد غنام : المرجع السابق، ص 219 وما يليها.

الاختصاص والولاية بنظر بعض المنازعات المحددة[1]، ومنها جرائم تقنية المعلومات والاتصالات.

وكذلك الشأن فى التشريع الفرنسى وفقاً لآخر التعديلات التشريعية الواردة بقانون الإجراءات الجنائية. حيث تنص المادة (704) من قانون الإجراءات الجنائية الفرنسي- المعدلة بالقانون رقم 1598 لسنة 2007 - على أن تنشأ فى دائرة كل محكمة استئناف محكمة جنح أو أكثر للتحقيق والحكم فى الجرائم المنصوص عليها فى بعض القوانين الاقتصادية[2]. ومنها بالطبع جرائم تقنية المعلومات، وجرائم الملكية الفكرية.

وأخيراً فقد تنبه المشرع المصرى لمبدأ التخصص القضائي، فأنشأ المحاكم

---

(1) راجع : قانون المحاكم الاقتصادية لجمهورية روسيا البيضاء الصادر بموجب القانون رقم (217) الصادر فى كانون الأول ديسمبر سنة 1998 والذى اعتمده مجلس النواب فى الأول من نوفمبر 1998 والذى دخل حيز النفاذ فى 26 نوفمبر 1998.

ЗАКОН РЕСПУБЛИКИ БЕЛАРУСЬ от 9 декабря 1998 г. N 217-З О ХОЗЯЙСТВЕННЫХ СУДАХ В РЕСПУБЛИКЕ БЕЛАРУСЬ Принят Палатой представителей 10 ноября 1998 годаОдобрен Советом Республики 26 ноября 1998 года

(2) Article 704-1 En savoir plus sur cet article... Modifié par Loi n°2004-204 du 9 mars 2004 - art. 21 JORF 10 mars 2004 en vigueur le 1er octobre 2004Le tribunal de grande instance de Paris a seul compétence pour la poursuite, l'instruction et le jugement des délits prévus aux articles L. 465-1 et L. 465-2 du code monétaire et financier. Cette compétence s'étend aux infractions connexes. Le procureur de la République et le juge d'instruction de Paris exercent leurs attributions sur toute l'étendue du territoire national.

الاقتصادية الجنائية بموجب القانون رقم 120 لسنة 2008، لتختص دون غيرها بنظر منازعات بعينها[1]، ووفقاً لما نصت عليه المادة رقم (4) من قانون إنشائها فإن اختصاصها يشمل نظر الدعاوى الجنائية الناشئة عن قانون تنظيم التوقيع الالكتروني، وقانون تنظيم الاتصالات.

ونأمل من المشرع الإماراتى أن ينتهج مبدأ التخصص القضائى فى مجال جرائم تقنية المعلومات والاتصالات، وغيرها من الجرائم ذات الصلة أو المرتبطة بهذه الجرائم. حيث لا تثير فكرة إنشاء قضاء متخصص ثمة مشكلات قانونية، إذا راعى المشرع فى قانون إنشائها، توافق هذه المحاكم واختصاصها مع المبادئ والقواعد الدستورية، بحيث يكون إنشائها بناء على قانون، وأن تتوافق مع مبدأ وحدة واستقلالية القضاء، بل ونؤكد هنا أن التخصص القضائى يأتى متوافقاً مع ما جرت عليه توصيات مؤتمر روما قديما منذ سنة 1953 الذى حث ضمن توصياته على أن يراعى المشرع فى كل محكمة تخصيص عدد من قضاتها لمسائل معينة[2].

---

(1) القانون رقم 120 لسنة 2008 بإصدار قانون إنشاء المحاكم الاقتصادية فى مصر، الجريدة الرسمية، العدد 21 تابع فى 22 مايو 2008.

(2) راجع : مجموعة المناقشات والقرارات الصادرة عن المؤتمر الدولى السادس لقانون العقوبات، المجلة الدولية لقانون العقوبات، سنة 1953، ص 300 وما بعدها.

الخــاتمـة

حاولنا من خلال هذه الدراسة التعرف على جرائم الاعتداء على الأمـن الالكـتروني، وخطورتهـا، وانعكاسـاتها المختلفـة، وكـذلك استكشـاف أوجـه قصـور قواعـد الحمايـة الجنائية بشقيها (الموضوعى والإجرائي) فى هذا المجال الحيوي، بهدف التوصل إلى رسـم معالم النموذج التشريعى الأمثل للمصالح محل الحماية الجنائية. وقد خلصنا من خلال هذه الدراسة إلى التوصيات التالية :-

(1) من المناسب، أن يجرى نص المادة رقم (50) من مرسوم بقانون اتحادى رقم (5) لسنة 2012 فى شأن مكافحة جرائم تقنية المعلومات، وكذلك نص المادة رقـم (23) من مرسوم بقانون اتحادى رقم (3) بشأن إنشاء الهيئة الوطنية للأمـن الالكـترونى عـلى النحو التالى " لا يسرى فى شأن هذا القانون أى حكم يتعارض مع أحكامـه ". بـدلاً مـن النص على أنه " يلغى كل حكم يخالف، أو يتعارض مع أحكام هـذا المرسـوم بقـانون". حتى يتحقق الموائمة التشريعية خصوصاً عند وجود تعارض محتمل بين هذه القوانين - وهى من القوانين الخاصة - وبين القواعد أو النصوص العامة، التى تقرر ذات الحمايـة لمصلحة جوهرية (موضوعية أو إجرائية) للأمن الالكتروني.

(2) من الملائم، أن ينص المشرع الإماراتى على تجريم صـور الاعتـداء عـلى الأمـن الالكترونى التى تتم عن طريق الامتناع الـذى تعقبـه نتيجـة ايجابيـة ناشـئة عـن هـذا الامتناع من ذلك مثلاً إحجام أو امتناع الجهة أو الشخص عن اتخاذ سبل تأمين وحماية الشبكة المعلوماتية، أو شبكة الاتصالات، أو نظم المعلومات، إذا ترتب على ذلـك أضرار أو أخطار معينة، تهدد المصالح ذات الأهمية. مع مراعاة النص على الشروط والضوابط الأخرى لانعقاد المسؤولية عن هذه الأفعال، كأن يكون هناك واجب أو التزام قانونى أو تعاقدى على الجهة أو الشخص المسئول، بشأن التأمين والحماية، وأن يكون لديـه إرادة هذا الامتناع، مع توافر علاقة السببية بين الامتناع والنتيجة المعاقب عليها.

(3) من الضروري، أن يحصر المشرع الإمـاراتى تطلـب القصـد الخـاص فى جـرائم الاعتداء على الأمن الالكترونى فى أضيق الحدود، فالنص على ضرورة وجود غايـة معينـة أو مسار بعيد تسلكه إرادة الجانى أبعد مما هو عليه فى القصد العـام، كثـيرا ينهـار بـه البنيان القانونى للجريمة بتخلفه، ولا يتبقى شئ يسأل عنه الجاني، كما لو تخلفت لديـه نية الإلغاء، أو الإتلاف، أو التعديل، فى جريمة دخول موقع الكترونى أو نظام معلوماتي.

(4) مـن الملائـم، أن يتبـع المشرع الإمـاراتى ذات المسـلك الـذى تتجـه إليـه اغلـب التشريعـات الحديثـة، بشـأن الـنص صراحـة عـلى تجـريم الاعتـداء غـير

العمدى على المصالح محل الحماية الجنائية فى نطاق الاعتداء على الأمن الالكتروني، ذلك لأن هناك بعض الحالات التى يدخل فيها مرتكب الفعل إلى الأنظمة المعلوماتية وقد تكون (بغير عمد)، ومع ذلك ينتج عنها أضرار جسيمة، تلحق بأنظمة المعلومات وخصوصاً ما يتعلق منها بالأمن القومي، أو مصلحة الدولة الاقتصادية، أو علاقاتها الدولية والإقليمية، على أن يركز المشرع بصفة خاصة على تجريم حالات (الخطأ الواعى أو الخطأ مع التوقع أو مع التبصر)، حيث يتوقع الجانى حدوث النتيجة بدرجة كبيرة عما هو عليه الشأن فى (الخطأ غير الواعي).

(5) من المناسب، فى تقرير الجزاءات المقررة لجرائم الاعتداء على الأمن الالكتروني، أن ينص المشرع الإماراتى على تشديد بعض العقوبات أو التدابير فى حالة (العود للجريمة). وكذلك النص على ضرورة نشر الحكم الصادر بالإدانة.

(6) من الملائم، أن ينتهج المشرع الإماراتى مبدأ التخصص القضائى فى مجال جرائم تقنية المعلومات والاتصالات، وما يرتبط بها من جرائم لا تقبل التجزئة، وذلك على نهج ما سارت عليه أغلب التشريعات المقارنة، كالتشريع البيلاروسي، والمشرع الفرنسي، والمشرع المصري.

المراجــع

أولاً : المراجع العربية :

(أ) المؤلفـات العامـة :

- **د. احمد شوقى عمر أبو خطوة :**

  - المبادئ العامة فى قانون الإجراءات الجنائية، القاهرة، 2011.
  - شرح الأحكام العامة لقانون العقوبات، الجزء الأول، النظرية العامـة للجريمـة، دار النهضة العربية، القاهرة، 1999.

- د. عبد الرءوف مهدى : شرح القواعد العامة لقانون العقوبات، القاهرة، 2004.
- د. عبد العظيم مرسى وزير : شرح قـانون العقوبـات، القسـم العـام، الجـزء الأول، النظرية العامة للجريمة، الطبعة الرابعة، دار النهضة العربية، القاهرة، 2006.
- د. مأمون محمد سـلامة : قـانون العقوبـات، القسـم العـام، دار النهضـة العربيـة، القاهرة، 1996.
- د. محمد عيـد الغريـب : شرح قـانون العقوبـات القسـم العـام، النظريـة العامـة للعقوبة والتدابير الاحترازية، بدون دار نشر، القاهرة، 1999-2000.

- د. محمود محمود مصطفى : شرح قانون الإجراءات الجنائية، الطبعة الثانية عشرة، القاهرة، 1988.

(ب) المؤلفات الخاصة :

- د. أحمد شوقى عمر أبو خطوة : جرائم التعريض للخطر العام، دراسة مقارنة، دار النهضة العربية، القاهرة، 1999.
- د. أحمد عوض بلال : محاضرات فى الجزاء الجنائي، دار النهضة العربية، القاهرة، 2000 - 2001.
- د. السعيد مصطفى السعيد : مجموعة المحاضرات التى ألقيت على طلبة الدراسات العليا فى الجرائم الاقتصادية، 1967.
- د. أمين مصطفى محمد : النظرية العامة لقانون العقوبات الإدارى (ظاهرة الحد من العقاب)، دار الجامعة الجديدة للنشر، الإسكندرية،1996.
- د. حاتم بكار : حماية حق المتهم فى محاكمة عادلة، دراسة تحليلية تأصيلية انتقاديه مقارنة، منشأة المعارف، الإسكندرية، 1997.
- د. حسنى أحمد الجندى : القانون الجنائى للمعاملات التجارية، الكتاب الأول، القانون الجنائى للشركات، دار النهضة العربية، القاهرة، 1989.

- د. شريف سيد كامل : تعليق على قانون العقوبات الفرنسى الجديد، القسم العام، الطبعة الأولي، دار النهضة العربية، القاهرة، 1998.
- د. عبد الفتاح مصطفى الصيفى : القاعدة الجنائية، دراسة تحليلية لها على ضوء الفقه الجنائى المعاصر، دار النهضة العربية، القاهرة، بدون سنة نشر.
- **د. غنام محمد غنام :**
  - الحماية الجنائية للادخار فى شركات المساهمة، دار النهضة العربية، القاهرة، 1988.
  - دور قانون العقوبات فى مكافحة جرائم الكمبيوتر والانترنت وجرائم الاحتيال المنظم باستعمال شبكة الانترنت، دار الفكر والقانون، المنصورة، مصر، 2010.
- د. محمود عبد العزيز محمد السيد الشريف : مدى ملائمة الجزاءات الجنائية الاقتصادية فى ظل السياسة الجنائية المعاصرة، النظرية العامة للجزاء الجنائى الاقتصادي، دراسة تحليلية تأصيلية مقارنة، دار النهضة العربية، القاهرة، 2006-2007.
- د. محمود كبيش : المسئولية الجنائية لمراقب الحسابات فى شركات المساهمة، دراسات مقارنة فى القانونين المصرى والفرنسي، دار النهضة العربية، القاهرة، 1992.

- د. محمود محمود مصطفى : الجرائم الاقتصادية فى القانون المقارن، الجـزء الأول، الأحكام العامة والإجراءات الجنائية، الطبعة الثانية، القاهرة، 1979.

- **د. محمود نجيب حسنى :**

- علاقة السببية، دار النهضة العربية، القاهرة، 1984

- النظرية العامة للقصد الجنائي، دراسة تأصيلية مقارنة للـركن المعنـوى فى الجـرائم العمدية، الطبعة الثالثة، دار النهضة العربية، القاهرة، 1988.

- جــرائم الامتنــاع والمســئولية الجنائيــة عــن الامتنــاع، دار النهضــة العربيــة، القاهرة،1986.

- دروس فى القانون الجنائى الدولي، دار النهضة العربية، القاهرة، 1959-1960.

- د. مزهر جعفر عبد السـلام : جريمـة الامتنـاع، الطبعـة الأولى، الإصـدار الأول، دار الثقافة للنشر والتوزيع، عمان، الأردن، 1999.

- د. مصطفى كامل كيره : الجرائم الاقتصادية، دار النهضة العربية، 1983.

- د. مصطفى منير : جـرائم إسـاءة اسـتعمال السـلطة الاقتصـادية، الهيئـة المصريـة العامة للكتاب، 1992.

(جـ) رسائل الدكتوراه :

- د. عبد الرءوف مهدى : المسـئولية الجنائيـة عـن الجـرائم الاقتصـادية، فى القـانون المقارن، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، 1974.
- د. عبد المنعم محمد إبراهيم رضوان : موضع الضرر فى البنيـان القـانونى للجريمـة، دراسة تحليلية تأصيلية، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، 1994.
- د. نائله عادل محمد فريـد قـورة : جـرائم الحاسـب الاقتصـادية، دراسـة نظريـة تطبيقية، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، 2013.

(د) أبحاث ومؤتمرات :

- خبير/ عبد الناصر محمد محمود فرغلى ، د. محمد عبيد سيف سعيد المسمارى : الإثبات الجنائى بالأدلة الرقمية من الناحيتين القانونية والفنيـة، دراسـة تطبيقيـة مقارنة، المؤتمر العربى الأول لعلوم الأدلة الجنائية والطـب الشرعـي، الريـاض، 2-11/4/ 1428هـ - الموافق 12-2007/11/14م.

ثانياً : المرجع الأجنبية :

- **A. Vitu** : La protection pénal de l'interet public et l'interet des associes dans les sociétés commerciales et civiles " Rapport pressente aux cinquième journées juridiques Franco-italienne, Paris , Nancy , 5 – 10 juin 1967.
- **A. Wlener,** theory of economic criminal law Hungarian national group of international association of penal law Budapest 1984 London 1986.
- **Maris Cremona, Jonathan Herring MA**, Criminal law, Macmilan, 1998.
- **Merle et vitu** : trait de droit criminel , quatrième édition , 1981.
- **Merle- Vitu** : Procedure Pénal, 1984.
- Rotman " L'evolutuion de la pense juridique sur le but de la sanction penale Melange Ancel , 1975.
- **Stefani, Levasseur, Bouloc :** Procedure Penal, 1984.
- **U.S. c.Maxwell 45 MJ** 406 , 1996; Rene PEPIN, Le statut juridique du cornel au Canada et aux Etats- Unis, www. Lex-electronica. Org/articles/v 2-6/pepin.htm
- United States V. Smith, 27 F. Supp. 2d 111, 16-1115 (C.D. III. 1998). www.cybercrime.gov/smanual 2002.htm

الفهرس

الموضوع	الصفحة



dar.elfker@hotmail.com